Acronis®
COMPUTE WITH CONFIDENCE
WWW.ACRONIS.PL

Acronis® Backup & Recovery 10™ Advanced Server Virtual Edition

Update 5

Podręcznik użytkownika

Spis treści

1 Wprowadzenie do programu Acronis® Backup & Recovery™ 10

1.1 Omówienie programu Acronis Backup & Recovery 10

Program Acronis Backup & Recovery 10, oparty na opatentowanych technologiach firmy Acronis do tworzenia obrazów dysku i przywracania systemu od podstaw, zastępuje program Acronis True Image Echo jako rozwiązanie nowej generacji do odzyskiwania danych po awarii.

Produkt Acronis Backup & Recovery 10 Advanced Server Virtual Edition posiada te same zalety, co rodzina produktów Acronis True Image Echo:

- Tworzenie kopii zapasowej całego dysku lub woluminu, w tym systemu operacyjnego, wszystkich aplikacji i danych
- Odzyskiwanie danych na dowolny komputer bez zainstalowanego systemu operacyjnego
- Tworzenie kopii zapasowej plików i folderów oraz ich odzyskiwanie
- Skalowalność od jednego komputera do poziomu całego przedsiębiorstwa
- Obsługa środowisk z systemem Windows i Linux
- Scentralizowane zarządzanie rozproszonymi stacjami roboczymi i serwerami
- Specjalne serwery do optymalizacji zasobów pamięci masowej

Program Acronis Backup & Recovery 10 Advanced Server Virtual Edition oferuje nowe funkcje ułatwiające organizacjom spełnienie celów w zakresie czasu odtworzenia po awarii, zmniejszając zarówno wydatki na środki trwałe, jak i koszty obsługi oprogramowania.

- **Wykorzystanie istniejącej infrastruktury IT**

  Deduplikacja danych, zmniejszająca koszty pamięci masowej i wykorzystanie przepustowości sieci

  Elastyczny mechanizm deduplikacji, umożliwiający deduplikację danych kopii zapasowych zarówno w źródle, jak i w magazynie

  Ulepszona obsługa automatycznych bibliotek taśm

  Kompatybilność wstecz i łatwa aktualizacja z programu Acronis True Image Echo

- **Wysoce zautomatyzowana ochrona danych**

  Wszechstronne planowanie ochrony danych (tworzenie kopii zapasowych, przechowywanie i sprawdzanie poprawności) w ramach zasad tworzenia kopii zapasowych

  Wbudowane schematy tworzenia kopii zapasowych Wieża Hanoi i Dziadek-ojciec-syn z możliwością dostosowania parametrów

  Szeroki wybór zdarzeń i warunków powodujących tworzenie kopii zapasowych

- **Zarządzanie scentralizowane na podstawie zasad**

  Stosowanie zasad tworzenia kopii zapasowych do grup komputerów

  Statyczne i dynamiczne grupowanie komputerów

  Grupowanie komputerów fizycznych lub maszyn wirtualnych

- **Wygodna praca w środowiskach wirtualnych**

  Tworzenie kopii zapasowych maszyn wirtualnych i ich odzyskiwanie bez konieczności instalacji specjalnego oprogramowania na każdej maszynie

  konwersja kopii zapasowej na w pełni skonfigurowaną maszynę wirtualną VMware, Microsoft, Parallels, Citrix lub Red Hat KVM.
- **Nowa struktura graficznego interfejsu użytkownika**

  Pulpit nawigacyjny do szybkiego podejmowania decyzji operacyjnych

  Przegląd wszystkich skonfigurowanych i wykonywanych operacji oraz oznaczanie kolorami operacji zakończonych powodzeniem i niepowodzeniem
- **Zabezpieczenia niezbędne w przedsiębiorstwie**

  Kontrola praw użytkowników do wykonywania operacji i uzyskiwania dostępu do kopii zapasowych

  Uruchamianie usług z minimalnymi prawami użytkownika

  Ograniczony dostęp zdalny do agenta tworzenia kopii zapasowych

  Bezpieczna komunikacja między komponentami programu

  Uwierzytelnianie komponentów przy użyciu certyfikatów innych firm

  Opcje szyfrowania danych zarówno podczas ich przesyłania, jak i magazynowania

  Tworzenie kopii zapasowych komputerów zdalnych w centralnym węźle magazynowania za zaporą

1.2 Rozpoczęcie pracy

Zarządzanie bezpośrednie

1. Zainstaluj konsolę zarządzania Acronis Backup & Recovery 10 Management Console i komponent Acronis Backup & Recovery 10 Agent.
2. Uruchom konsolę.

   Windows

   Uruchom konsolę, wybierając ją z menu Start.

   Linux

   Zaloguj się jako użytkownik root lub jako zwykły użytkownik i zmień użytkownika w razie potrzeby. Uruchom konsolę, korzystając z polecenia

   ```
   /usr/sbin/acronis_console
   ```
3. Podłącz konsolę do komputera, na którym jest zainstalowany agent.

Dokąd przejść z tego miejsca

Aby uzyskać dalsze instrukcje, zobacz „Podstawowe pojęcia (s. 30)”.

Aby zapoznać się z elementami graficznego interfejsu użytkownika, zobacz „Korzystanie z konsoli zarządzania (s. 11)”.

Aby dowiedzieć się, jak umożliwić użytkownikom innym niż root uruchamianie konsoli w systemie Linux, zobacz „Uprawnienia do połączeń lokalnych (s. 87)”.

Aby dowiedzieć się, jak umożliwić nawiązywanie połączenia zdalnego z komputerem z systemem Linux, zobacz „Uprawnienia do połączeń zdalnych w systemie Linux (s. 88)”.

Zarządzanie scentralizowane

Zalecamy, aby najpierw wypróbować zarządzanie jednym komputerem przy użyciu funkcji zarządzania bezpośredniego, zgodnie z powyższym opisem.

Aby rozpocząć zarządzanie scentralizowane:

1. Zainstaluj serwer zarządzania Acronis Backup & Recovery 10 Management Server (s. 21).
2. Zainstaluj komponenty Acronis Backup & Recovery 10 Agent na komputerach wymagających ochrony danych. Podczas instalowania agentów zarejestruj każdy komputer na serwerze zarządzania. W tym celu wprowadź adres IP lub nazwę serwera i poświadczenia administratora centralnego w jednym z okien kreatora instalacji.
3. Zainstaluj konsolę zarządzania Acronis Backup & Recovery 10 Management Console (s. 24) na preferowanym komputerze. Jeśli do wyboru są konsole instalowane w systemach Windows i Linux, zalecamy wybór konsoli dla systemu Windows. Zainstaluj generator Acronis Bootable Media Builder.
4. Uruchom konsolę. Utwórz nośnik startowy.
5. Podłącz konsolę do serwera zarządzania.

Uproszczony sposób zarządzania scentralizowanego

- **Kopia zapasowa**

Korzystając z opcji **Utwórz kopię zapasową**, wybierz komputer, którego kopię zapasową chcesz utworzyć, a następnie utwórz plan tworzenia kopii zapasowych (s. 425) na tym komputerze. Plany tworzenia kopii zapasowych można utworzyć kolejno na wielu komputerach.

- **Odzyskiwanie**

Korzystając z opcji **Odzyskaj**, wybierz komputer, którego dane chcesz odzyskać, i utwórz zadanie odzyskiwania na tym komputerze. Zadania odzyskiwania można utworzyć kolejno na wielu komputerach.

Aby odzyskać zawartość całego komputera lub cały system operacyjny, którego nie można uruchomić, należy użyć nośnika startowego (s. 424). Operacji wykonywanych przy użyciu nośnika startowego nie można kontrolować na serwerze zarządzania, ale można odłączyć konsolę od serwera i połączyć ją z komputerem uruchomionym przy użyciu nośnika.

- **Zarządzanie planami i zadaniami**

Aby zarządzać planami i zadaniami istniejącymi na komputerach zarejestrowanych, wybierz kolejno **Komputery > Wszystkie komputery** w drzewie **Nawigacja**, a następnie wybierz każdy komputer po kolei. Na panelu **Informacje** zostaną wyświetlone informacje o stanie oraz szczegóły dotyczące planów i zadań istniejących na każdym komputerze, na podstawie których można uruchomić, zatrzymać, zmodyfikować i usunąć plany oraz zadania.

Można również skorzystać z widoku **Zadania**, w którym są wyświetlane wszystkie zadania istniejące na komputerach zarejestrowanych. Zadania można filtrować według komputerów, planów tworzenia kopii zapasowych i innych parametrów. Szczegółowe informacje znajdują się w pomocy kontekstowej.

- **Przeglądanie dziennika**

Aby przejrzeć dziennik scentralizowany zawierający dane zebrane z komputerów zarejestrowanych, wybierz pozycję **Dziennik** w drzewie **Nawigacja**. Wpisy dziennika można filtrować według komputerów, planów tworzenia kopii zapasowych i innych parametrów. Szczegółowe informacje znajdują się w pomocy kontekstowej.

- **Tworzenie skarbców centralnych**

Po wybraniu opcji przechowywania wszystkich archiwów kopii zapasowych w jednej lub kilku lokalizacjach sieciowych należy utworzyć w tych lokalizacjach skarbce centralne. Po utworzeniu skarbca można przeglądać jego zawartość i zarządzać nią, wybierając kolejno pozycje **Skarbce > Centralne > „Nazwa skarbca”** w drzewie **Nawigacja**. Skrót do skarbca zostanie wdrożony na wszystkich komputerach zarejestrowanych. Skarbiec można wskazać jako miejsce docelowe kopii zapasowych w dowolnym planie tworzenia kopii zapasowych utworzonym przez siebie lub przez użytkowników komputerów zarejestrowanych.

Zaawansowany sposób zarządzania scentralizowanego

Aby najlepiej wykorzystać funkcje zarządzania scentralizowanego dostępne w programie Acronis Backup & Recovery 10, należy wybrać następujące opcje:

- **Korzystanie z deduplikacji**
  1. Zainstaluj węzeł magazynowania Acronis Backup & Recovery 10 Storage Node (s. 22) i dodaj go do serwera zarządzania.
  2. Utwórz zarządzany skarbiec deduplikacji w węźle magazynowania.
  3. Zainstaluj dodatek deduplikacji firmy Acronis do agenta na wszystkich komputerach, których kopie zapasowe będą tworzone w skarbcu deduplikacji.
  4. Upewnij się, że utworzone plany tworzenia kopii zapasowych korzystają ze skarbca zarządzanego jako miejsca docelowego dla archiwów kopii zapasowych.
- **Tworzenie zasad zamiast planów tworzenia kopii zapasowych**

Skonfiguruj scentralizowane zasady tworzenia kopii zapasowych i zastosuj je w grupie **Wszystkie komputery**. W ten sposób plany tworzenia kopii zapasowych zostaną wdrożone na wszystkich komputerach przez wykonanie jednej czynności. Wybierz kolejno **Czynności > Utwórz zasady tworzenia kopii zapasowych** w górnym menu, a następnie skorzystaj z pomocy kontekstowej.

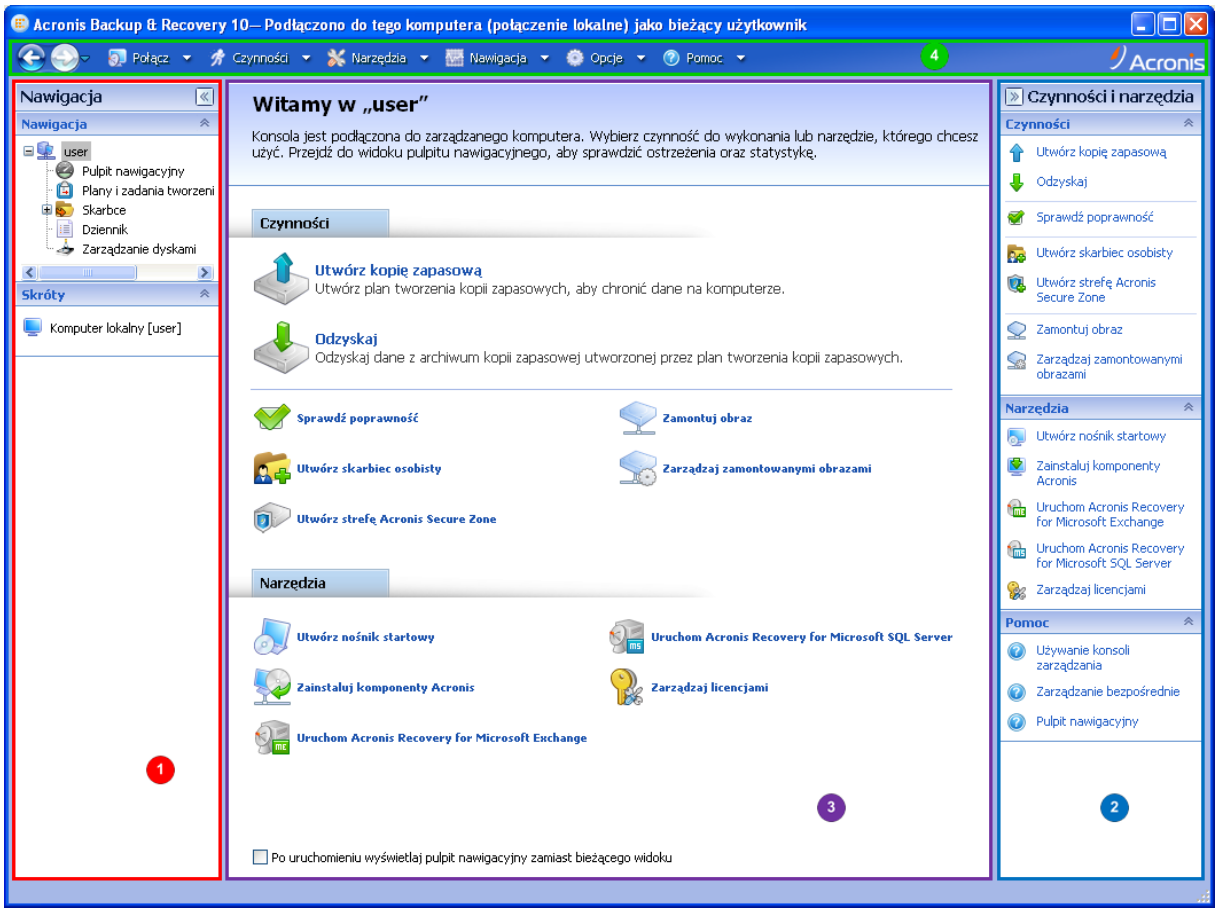
- **Grupowanie komputerów zarejestrowanych na serwerze zarządzania**

Na podstawie odpowiednich parametrów połącz komputery zarejestrowane w grupy, utwórz kilka zasad i zastosuj każdą z nich do właściwej grupy komputerów. Aby uzyskać więcej informacji, zobacz sekcję „Grupowanie zarejestrowanych komputerów (s. 70)”.

Obszerny przykład zaawansowanego zarządzania scentralizowanego przedstawiono w sekcji „Konfigurowanie scentralizowanej ochrony danych w sieci heterogenicznej (s. 67)”.

1.2.1 Używanie konsoli zarządzania

Po połączeniu konsoli z komputerem zarządzanym (s. 423) lub serwerem zarządzania (s. 427) w jej obszarze roboczym (w menu, obszarze głównym z ekranem **Witamy**, panelu **Nawigacja**, panelu **Czynności i narzędzia**) pojawią się odpowiednie elementy umożliwiające wykonanie operacji przy użyciu agenta lub operacji przy użyciu serwera.



Konsola zarządzania Acronis Backup & Recovery 10 Management Console — ekran Witamy

Główne elementy obszaru roboczego konsoli

	Nazwa	Opis
1	Panel **Nawigacja**	Zawiera drzewo **nawigacji** i pasek **skrótów** oraz umożliwia nawigację do innych widoków (zobacz sekcję Panel nawigacji (s. 12)).
2	Panel **Czynności i narzędzia**	Zawiera paski z zestawem czynności, które można wykonać, i narzędzi (zobacz sekcję Panel Czynności i narzędzia (s. 14)).
3	Obszar **główny**	Główne miejsce pracy, w którym tworzy się i modyfikuje plany, zasady i zadania tworzenia kopii zapasowych oraz zarządza nimi, a także wykonuje inne operacje. Zawiera różne widoki i strony czynności (s. 16) w zależności od elementów wybranych w menu, drzewie **nawigacji** lub panelu **Czynności i narzędzia**.
4	Pasek **menu**	Pojawia się u góry okna programu i umożliwia wykonywanie wszystkich operacji, które są dostępne na obu panelach. Elementy menu zmieniają się dynamicznie.

Do komfortowej pracy z konsolą zarządzania jest wymagana rozdzielczość ekranu 1024 x 768 lub wyższa.

Panel „Nawigacja"

Na panelu nawigacji znajduje się drzewo **nawigacji** i pasek **skrótów**.

Drzewo nawigacji

Drzewo **nawigacji** umożliwia przechodzenie między widokami programu. Dostępne widoki zależą od tego, czy konsola jest połączona z komputerem zarządzanym czy serwerem zarządzania.

Widoki dotyczące komputera zarządzanego

Po połączeniu konsoli z komputerem zarządzanym w drzewie nawigacji będą dostępne następujące widoki.

- **[Nazwa komputera]**. Korzeń drzewa zwany również widokiem **powitalnym**. Jest w nim wyświetlana nazwa komputera, z którym jest aktualnie połączona konsola. Widok ten umożliwia uzyskanie szybkiego dostępu do głównych operacji dostępnych na komputerze zarządzanym.
  - **Pulpit nawigacyjny**. Ten widok służy do szybkiej oceny, czy dane na komputerze zarządzanym są skutecznie chronione.
  - **Plany i zadania tworzenia kopii zapasowych**. Ten widok służy do zarządzania planami i zadaniami tworzenia kopii zapasowych na komputerze zarządzanym: uruchamiania, edycji, zatrzymywania i usuwania planów oraz zadań, wyświetlania ich stanu i statusu oraz monitorowania planów.
  - **Skarbce**. Ten widok służy do zarządzania skarbcami osobistymi i przechowywanymi w nich archiwami, dodawania nowych skarbców, zmiany nazwy i usuwania istniejących, sprawdzania poprawności skarbców, przeglądania zawartości kopii zapasowej, montowania kopii zapasowych jako urządzeń wirtualnych itd.
  - **Dziennik**. Ten widok służy do analizowania informacji na temat operacji wykonywanych przez program na komputerze zarządzanym.
  - **Zarządzanie dyskami**. Ten widok służy do wykonywania operacji na dyskach twardych komputera.

Widoki dotyczące serwera zarządzania

Po połączeniu konsoli z serwerem zarządzania w drzewie nawigacji będą dostępne następujące widoki.

- **[Nazwa serwera zarządzania]**. Korzeń drzewa zwany również widokiem **powitalnym**. Jest w nim wyświetlana nazwa serwera zarządzania, z którym jest aktualnie połączona konsola. Widok ten umożliwia uzyskanie szybkiego dostępu do głównych operacji dostępnych na serwerze zarządzania.
  - **Pulpit nawigacyjny**. Ten widok służy do szybkiej oceny, czy dane na komputerach zarejestrowanych na serwerze zarządzania są skutecznie chronione.
  - **Zasady tworzenia kopii zapasowych**. Ten widok służy do zarządzania zasadami tworzenia kopii zapasowych istniejącymi na serwerze zarządzania.
  - **Komputery fizyczne**. Ten widok służy do zarządzania komputerami zarejestrowanymi na serwerze zarządzania.
  - **Maszyny wirtualne**. Ten widok służy do zarządzania maszynami wirtualnymi z zarejestrowanych komputerów fizycznych oraz z komputerów zarejestrowanych z agentem dla maszyn ESX/ESXi.
  - **Skarbce**. Ten widok służy do zarządzania skarbcami centralnymi i przechowanymi w nim archiwami: tworzenia nowych skarbców zarządzanych i niezarządzanych, zmiany nazwy oraz usuwania istniejących skarbców.
  - **Węzły magazynowania**. Ten widok służy do zarządzania węzłami magazynowania. Węzeł magazynowania należy dodać, aby móc tworzyć skarbce centralne zarządzane przez węzeł.

- **Zadania**. Ten widok służy do zarządzania zadaniami, uruchamiania, edycji, zatrzymywania i usuwania zadań, monitorowania ich stanów oraz przeglądania ich historii.
- **Dziennik**. Ten widok służy do przeglądania historii operacji zarządzania scentralizowanego, takich jak tworzenie grupy jednostek zarządzanych, stosowanie zasad, zarządzanie skarbcem centralnym, jak również historii operacji zarejestrowanych w lokalnych dziennikach komputerów zarejestrowanych i węzłach magazynowania.

Pasek skrótów

Pasek **skrótów** znajduje się pod drzewem nawigacji. Umożliwia szybkie i wygodne nawiązywanie połączeń na żądanie z komputerami przez dodanie skrótów do nich.

Aby dodać skrót do komputera

1. Podłącz konsolę do komputera zarządzanego.
2. W drzewie nawigacji kliknij prawym przyciskiem myszy nazwę komputera (główny element drzewa nawigacji), a następnie wybierz polecenie **Utwórz skrót**.

   Jeśli konsola i agent są zainstalowane na tym samym komputerze, skrót do tego komputera zostanie dodany do paska skrótów automatycznie jako **Komputer lokalny [nazwa komputera]**.

   Jeśli konsola była już wcześniej połączona z serwerem zarządzania Acronis Management Server, skrót zostanie dodany automatycznie jako **AMS [nazwa komputera]**.

Panel „Czynności i narzędzia”

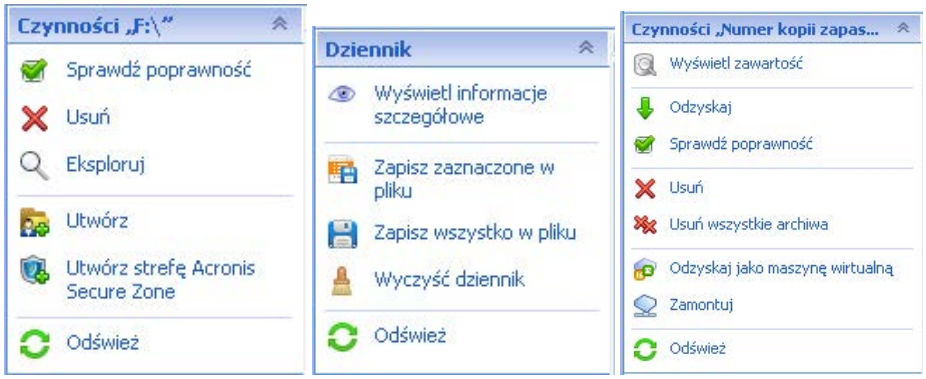
Panel **Czynności i narzędzia** umożliwia łatwą i efektywną pracę z programem Acronis Backup & Recovery 10. Paski na panelu zapewniają szybki dostęp do operacji i narzędzi programu. Wszystkie elementy paska **Czynności i narzędzia** są zduplikowane w menu programu.

Paski

Czynności: „[nazwa elementu]”

Zawiera zestaw czynności, które można wykonać na elementach wybranych w dowolnych widokach nawigacji. Kliknięcie czynności powoduje wyświetlenie odpowiedniej strony czynności (s. 17). Elementy z innych widoków nawigacji mają własne zestawy czynności. Nazwa paska zmienia się w zależności od wybranego elementu. Na przykład po wybraniu planu tworzenia kopii zapasowych o nazwie *Kopia zapasowa systemu* w widoku **Plany i zadania tworzenia kopii zapasowych** nazwa paska czynności zmieni się na **Czynności: „Kopia zapasowa systemu”** i dostępny będzie zestaw czynności typowych dla planów tworzenia kopii zapasowych.

Dostęp do wszystkich czynności można również uzyskać przy użyciu odpowiednich elementów menu. Element menu pojawi się na pasku menu po wybraniu elementu w dowolnym widoku nawigacji.

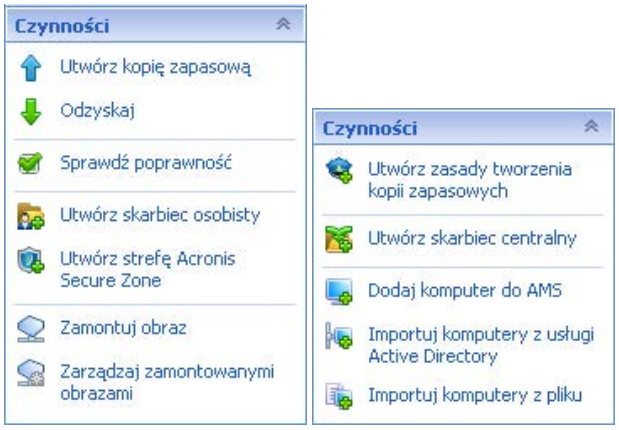


Przykłady paska „Czynności: [nazwa elementu]”

Czynności

Zawiera listę typowych operacji, które można wykonać na komputerze zarządzanym lub serwerze zarządzania. Jest identyczny dla wszystkich widoków. Kliknięcie operacji spowoduje wyświetlenie odpowiedniej strony czynności (zobacz sekcję Strony czynności (s. 17)).

Dostęp do wszystkich czynności można również uzyskać w menu **Czynności**.

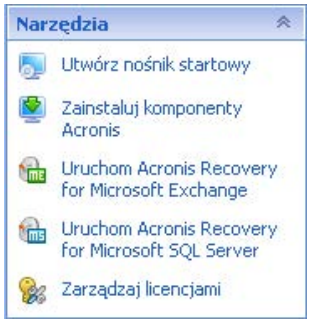


Pasek „Czynności" na komputerze zarządzanym i serwerze zarządzania

Narzędzia

Zawiera listę narzędzi Acronis. Identyczny we wszystkich widokach programu.

Dostęp do wszystkich narzędzi można także uzyskać za pomocą menu **Narzędzia**.



Pasek „Narzędzia"

Pomoc

Zawiera listę tematów pomocy. Różne widoki i strony czynności produktu Acronis Backup & Recovery 10 mają własne listy tematów pomocy.

Operacje na panelach

Rozwijanie/minimalizowanie paneli

Domyślnie panel **Nawigacja** jest rozwinięty, a panel **Czynności i narzędzia** — zminimalizowany. Być może trzeba będzie zminimalizować panel w celu zwolnienia miejsca w obszarze roboczym. W tym celu należy kliknąć pagon (- dla panelu **Nawigacja** lub - dla panelu **Czynności i narzędzia**). Panel zostanie zminimalizowany, a pagon zmieni swój kierunek. Kliknij go ponownie, aby rozwinąć panel.

Zmiana rozmiaru paneli

1. Wskaż obramowanie panelu.

2. Po zmianie wskaźnika na strzałkę dwukierunkową przeciągnij wskaźnik, aby przenieść obramowanie.

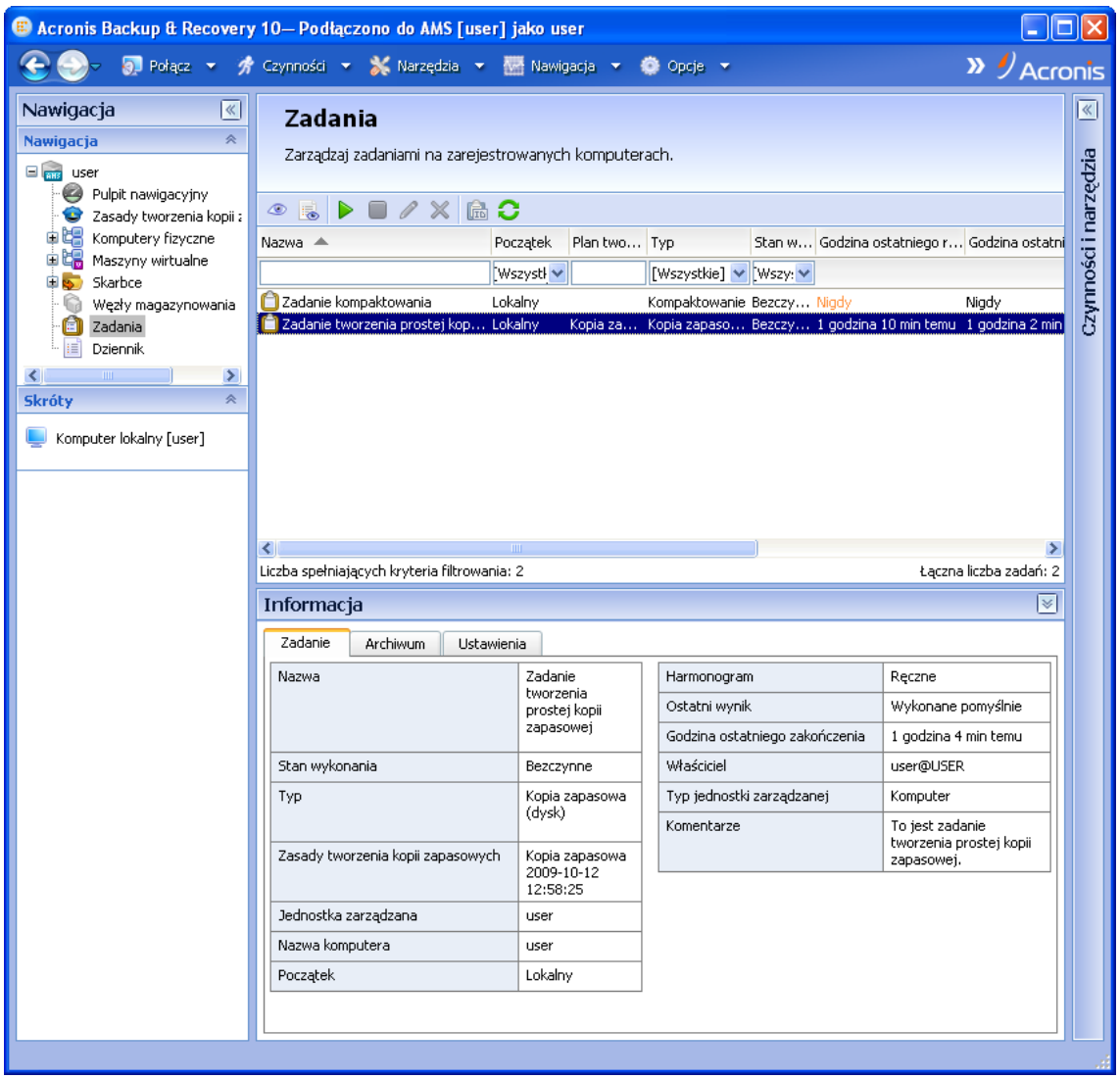
Konsola zarządzania „pamięta” ustawienie obramowania paneli. Po ponownym uruchomieniu konsoli zarządzania obramowanie paneli zostanie wyświetlone na tej samej pozycji, w której zostało ustawione poprzednio.

Obszar główny, widoki i strony czynności

Obszar główny to podstawowe miejsce pracy z konsolą. W tym miejscu można tworzyć i modyfikować plany, zasady, zadania tworzenia kopii zapasowych i zarządzać nimi, a także wykonywać inne operacje. W obszarze głównym są wyświetlane różne widoki i strony czynności, w zależności od elementów wybranych w menu, drzewie **Nawigacja** lub panelu **Czynności i narzędzia**.

Widoki

Widok pojawiający się w obszarze głównym po kliknięciu dowolnego elementu w drzewie **Nawigacja** na panelu nawigacji (s. 12).



Widok „Zadania”

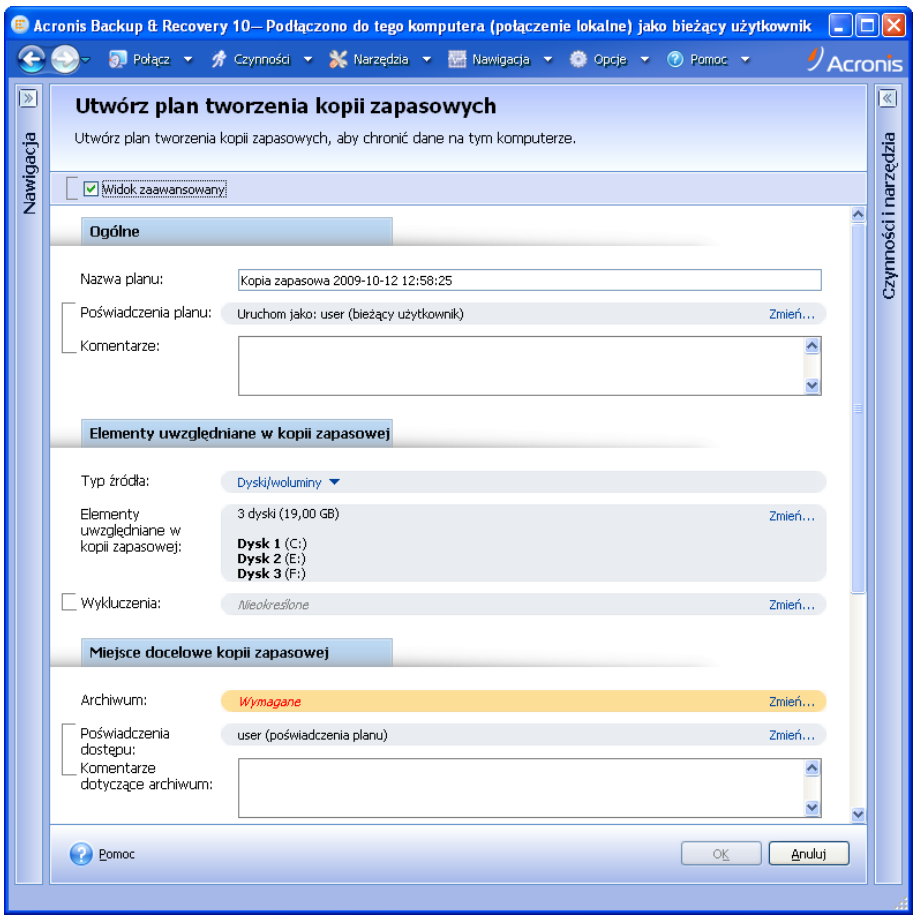
Typowy sposób pracy z widokami

Zwykle każdy widok zawiera tabelę elementów, pasek narzędzi tabeli z przyciskami oraz panel **Informacje**.

- Aby wyszukać wybrany element w tabeli, należy użyć funkcji filtrowania i sortowania.
- Wybierz żądany element w tabeli.
- Na panelu **Informacje** (domyślnie zwiniętym) wyświetl szczegóły dotyczące elementu.
- Wykonaj czynności na wybranym elemencie. Istnieje kilka sposobów wykonywania tej samej czynności na wybranych elementach:
  - kliknięcie przycisków na pasku narzędzi tabeli;
  - kliknięcie elementów na pasku **Czynności: [nazwa elementu]** (na panelu **Czynności i narzędzia**);
  - wybór elementów w menu **Czynności**;
  - kliknięcie elementu prawym przyciskiem myszy i wybór operacji w menu kontekstowym.

Strony czynności

Strona czynności pojawi się w obszarze głównym po kliknięciu dowolnego elementu czynności w menu **Czynności** lub na pasku **Czynności** w panelu **Czynności i narzędzia**. Zawiera listę kroków, które należy wykonać, aby utworzyć i uruchomić dowolne zadanie, plan tworzenia kopii zapasowych lub zasady tworzenia kopii zapasowych.

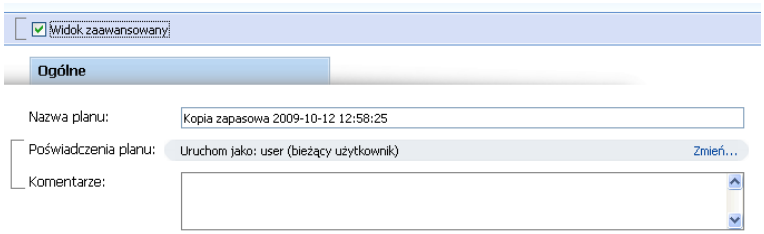


Strona czynności — Utwórz plan tworzenia kopii zapasowych

Korzystanie z formantów i określanie ustawień

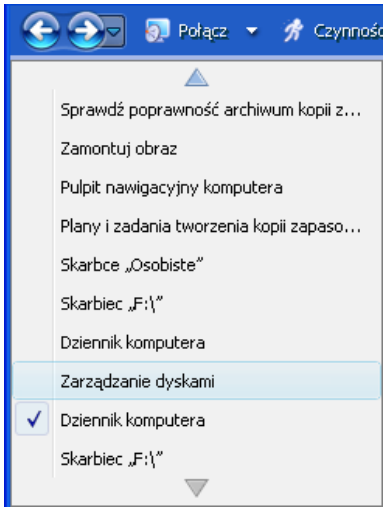
Strona czynności ma dwa widoki: podstawowy i zaawansowany. W widoku podstawowym ukryte są pola, takie jak poświadczenia, komentarze itd. Po włączeniu widoku zaawansowanego zostaną wyświetlone wszystkie dostępne pola. Między widokami można przełączać się, zaznaczając pole wyboru **Widok zaawansowany** u góry strony czynności.

Większość ustawień można skonfigurować, klikając odpowiednie łącze **Zmień…** po prawej stronie. Inne ustawienia należy wybrać na liście rozwijanej lub wpisać ich wartości w polach na stronie.



Strona czynności — Formanty

Program Acronis Backup & Recovery 10 zapamiętuje zmiany wprowadzone na stronach czynności. Na przykład po rozpoczęciu tworzenia planu tworzenia kopii zapasowych, a następnie nieukończeniu go i przełączeniu się z dowolnego powodu na inny widok, można kliknąć przycisk nawigacji **Wstecz** w menu. Ewentualnie, po wykonaniu kilku kroków, można kliknąć strzałkę **w dół** i wybrać na liście stronę, na której rozpoczęło się tworzenie planu. Dzięki temu można wykonać pozostałe kroki i ukończyć tworzenie planu tworzenia kopii zapasowych.



Pasek przycisków nawigacji — kontynuowanie operacji

1.3 Acronis Backup & Recovery 10 — komponenty

W tej sekcji znajduje się lista komponentów programu Acronis Backup & Recovery 10 z krótkim opisem ich funkcji.

Program Acronis Backup & Recovery 10 zawiera trzy główne typy komponentów.

Komponenty dla komputera zarządzanego (agenty)

Są to aplikacje służące do tworzenia kopii zapasowych, odzyskiwania danych i wykonywania innych operacji na komputerach zarządzanych przy użyciu programu Acronis Backup & Recovery 10. Do

wykonywania operacji na każdym komputerze zarządzanym agent potrzebuje licencji. Agenty mają wiele funkcji-dodatków oferujących dodatkowe możliwości, dlatego mogą wymagać dodatkowych licencji.

Za pomocą generatora nośnika startowego można tworzyć nośniki startowe, aby móc korzystać z agentów i innych narzędzi ratunkowych w środowisku ratunkowym. Dostępność dodatków do agentów w środowisku ratunkowym zależy od tego, czy dodatek jest zainstalowany na komputerze z generatorem nośników.

Komponenty do zarządzania scentralizowanego

Te komponenty, dostarczane z wersjami zaawansowanymi, umożliwiają zarządzanie scentralizowane. Korzystanie z tych komponentów nie wymaga licencji.

Konsola

Konsola ma graficzny interfejs użytkownika i umożliwia połączenie zdalne z agentami oraz innymi komponentami programu Acronis Backup & Recovery 10.

1.3.1 Agent dla systemu Windows

Agent ten umożliwia ochronę danych na poziomie dysków i na poziomie plików w systemie Windows.

Kopia zapasowa dysku

Ochrona danych na poziomie dysku polega na utworzeniu kopii zapasowej całego systemu plików dysku lub woluminu, wraz ze wszystkimi informacjami potrzebnymi do uruchomienia systemu operacyjnego, albo kopii zapasowej wszystkich sektorów dysku metodą „sektor po sektorze” (tryb „surowych” danych). Kopię zapasową danych dysku lub woluminu w postaci spakowanej określa się mianem kopii zapasowej dysku (woluminu) lub obrazem dysku (woluminu). Z takiej kopii zapasowej można odzyskać całe dyski lub woluminy, jak również poszczególne pliki lub foldery.

Kopia zapasowa plików

Ochrona danych na poziomie plików polega na utworzeniu kopii zapasowej plików i folderów znajdujących się na komputerze, na którym jest zainstalowany agent, lub w udziale sieciowym. Pliki można odzyskać w ich oryginalnej lokalizacji lub w innym miejscu. Odzyskać można wszystkie pliki i foldery znajdujące się w kopii zapasowej albo tylko wybrane z nich.

Inne operacje

Konwersja na maszynę wirtualną

Zamiast konwertować kopię zapasową dysku na plik dysku wirtualnego, co wymaga wykonania dodatkowych operacji przygotowujących dysk wirtualny do użytku, Agent dla systemu Windows wykonuje konwersję przez odzyskanie kopii zapasowej dysku na nową maszynę wirtualną jednego z następujących typów: VMware Workstation, Microsoft Virtual PC, Parallels Workstation, Citrix XenServer Open Virtual Appliance (OVA) lub Red Hat KVM. Pliki w pełni skonfigurowanej i działającej maszyny są umieszczane w folderze wybranym przez użytkownika. Można uruchomić maszynę przy użyciu odpowiedniego oprogramowania do wirtualizacji lub przygotować pliki maszyny w celu ich użycia w przyszłości.

Zarządzanie dyskami

Agent dla systemu Windows zawiera wygodne narzędzie do zarządzania dyskami pod nazwą Acronis Disk Director Lite. Operacje zarządzania dyskami, takie jak klonowanie dysków, konwertowanie

dysków, tworzenie, formatowanie i usuwanie woluminów, zmiana stylu partycjonowania dysku między MBR a GPT lub zmiana etykiety dysku, można wykonywać w systemie operacyjnym lub przy użyciu nośnika startowego.

Universal Restore

Dodatek Universal Restore na komputerze, na którym jest zainstalowany agent, umożliwia odzyskanie danych na sprzęt o innej konfiguracji oraz utworzenie nośnika startowego. Niweluje on różnice między urządzeniami istotnymi przy uruchamianiu systemu Windows, takimi jak kontrolery pamięci, płyta główna i mikroukład.

Deduplikacja

Ten dodatek umożliwia agentowi tworzenie kopii zapasowych w skarbcach deduplikacji zarządzanych przez węzeł magazynowania Acronis Backup & Recovery 10 Storage Node.

Agent for Hyper-V

Komponent Acronis Backup & Recovery 10 Agent for Hyper-V chroni maszyny wirtualne znajdujące się na serwerze wirtualizacji Hyper-V ESX(i). Agent umożliwia tworzenie kopii zapasowych maszyn wirtualnych z hosta bez konieczności instalowania agentów na każdej maszynie wirtualnej. Agenta instaluje się w systemie Windows 2008 Server x64 (w dowolnej wersji) lub Microsoft Hyper-V Server 2008 jako dodatek do komponentu Acronis Backup & Recovery 10 Agent for Windows.

Nie można zainstalować komponentu Acronis Backup & Recovery 10 Agent for Hyper-V przy użyciu licencji funkcji Acronis Online Backup.

W systemach-gościach muszą być zainstalowane usługi integracji (s. 56).

1.3.2 Agent dla systemu Linux

Agent ten umożliwia ochronę danych na poziomie dysków i na poziomie plików w systemie Linux.

Kopia zapasowa dysku

Ochrona danych na poziomie dysków polega na tworzeniu kopii zapasowej całego systemu plików dysku lub woluminu wraz ze wszystkimi informacjami potrzebnymi do uruchomienia systemu operacyjnego albo wszystkich sektorów dysku przy użyciu metody sektor po sektorze (tryb danych nieprzetworzonych). Kopia zapasowa dysku lub woluminu w postaci spakowanej to kopia zapasowa dysku (woluminu) lub obraz dysku (woluminu). Z takiej kopii zapasowej można odzyskać całe dyski lub woluminy, jak również poszczególne pliki lub foldery.

Kopia zapasowa plików

Ochrona danych na poziomie plików polega na tworzeniu kopii zapasowej plików i katalogów znajdujących się na komputerze, na którym jest zainstalowany agent, lub w udziale sieciowym udostępnionym przy użyciu protokołu smb lub nfs. Pliki można odzyskać do ich oryginalnej lokalizacji lub do innego miejsca. Odzyskać można wszystkie pliki i katalogi znajdujące się w kopii zapasowej albo tylko wybrane z nich.

Deduplikacja

Ten dodatek umożliwia agentowi tworzenie kopii zapasowych w skarbcach deduplikacji zarządzanych przez węzeł magazynowania Acronis Backup & Recovery 10 Storage Node.

1.3.3 Agent dla ESX/ESXi

Komponent Acronis Backup & Recovery 10 Agent dla ESX/ESXi chroni maszyny wirtualne znajdujące się na serwerze wirtualizacji VMware ESX lub ESXi. Agent umożliwia tworzenie kopii zapasowych maszyn wirtualnych z hosta bez konieczności instalowania agentów na każdej maszynie wirtualnej.

Agent jest dostarczany jako urządzenie wirtualne.

1.3.4 Komponenty do zarządzania scentralizowanego

W tej sekcji znajduje się lista komponentów poszczególnych wersji programu Acronis Backup & Recovery 10 umożliwiającego zarządzanie scentralizowane. Na wszystkich komputerach, na których dane mają być chronione, oprócz wspomnianych komponentów należy zainstalować również agentów programu Acronis Backup & Recovery 10.

Serwer zarządzania

Serwer zarządzania Acronis Backup & Recovery 10 Management Server to centralny serwer odpowiedzialny za ochronę danych w sieci przedsiębiorstwa. Serwer zarządzania to dla administratora:

- jeden punkt dostępu do infrastruktury Acronis Backup & Recovery 10;
- łatwy sposób ochrony danych na wielu komputerach (s. 423) przy użyciu zasad tworzenia kopii zapasowych (s. 433) i grupowania;
- funkcje monitorowania obejmujące całe przedsiębiorstwo;
- możliwość tworzenia skarbców centralnych (s. 428) do przechowywania archiwów kopii zapasowych (s. 419) przedsiębiorstwa;
- możliwość zarządzania węzłami magazynowania (s. 430).

Jeśli w sieci istnieje wiele serwerów zarządzania, działają one niezależnie, zarządzają innymi komputerami i zapisują archiwa w innych skarbcach centralnych.

Bazy danych serwera zarządzania

Serwer zarządzania korzysta z trzech baz danych Microsoft SQL:

- Baza danych konfiguracji zawiera listę zarejestrowanych komputerów i inne informacje dotyczące konfiguracji, w tym zasady tworzenia kopii zapasowych zdefiniowane przez administratora.
- Baza danych synchronizacji służy do synchronizacji serwera zarządzania z zarejestrowanymi komputerami i węzłami magazynowania. Jest to baza danych z bardzo szybko zmieniającymi się danymi operacyjnymi.
- Baza danych raportowania zawiera dziennik centralny. Ta baza danych może mieć bardzo duży rozmiar. Zależy on od ustawionego poziomu rejestrowania.

Bazy danych konfiguracji i synchronizacji powinny się znajdować na tym samym serwerze Microsoft SQL Server (zwanym serwerem operacyjnym) — najlepiej zainstalowanym na tym samym komputerze co serwer zarządzania. Bazę danych raportowania można umieścić na tym samym lub innym serwerze SQL.

Podczas instalowania serwera zarządzania należy określić zarówno serwery operacyjne, jak i serwery raportowania, z których będzie on korzystać. Dostępne są następujące opcje:

1. Program Microsoft SQL Server 2005 Express zawarty w pakiecie instalacyjnym i instalowany na tym samym komputerze. W takim przypadku na komputerze zostanie utworzona instancja serwera SQL z trzema bazami danych.
2. Program Microsoft SQL Server 2008 (dowolna wersja) zainstalowany wcześniej na dowolnym komputerze.
3. Program Microsoft SQL Server 2005 (dowolna wersja) zainstalowany wcześniej na dowolnym komputerze.

Integracja VMware vCenter

Jest to funkcja umożliwiająca przeglądanie maszyn wirtualnych zarządzanych przez serwer VMware vCenter Server w graficznym interfejsie użytkownika serwera zarządzania, wyświetlanie stanu tworzenia kopii zapasowych tych maszyn w programie vCenter oraz automatyczne rejestrowanie maszyn wirtualnych utworzonych przez program Acronis Backup & Recovery 10 w programie vCenter.

Integracja jest dostępna we wszystkich zaawansowanych wersjach produktu Acronis Backup & Recovery 10. Nie jest wymagana licencja wersji Virtual Edition. Na serwerze vCenter Server nie trzeba instalować żadnego oprogramowania.

Funkcja ta umożliwia ponadto automatyczne wdrażanie i konfigurowanie Agenta dla ESX/ESXi na dowolnym serwerze ESX/ESXi, który nie musi być zarządzany przez program vCenter.

Węzeł magazynowania

Węzeł magazynowania Acronis Backup & Recovery 10 Storage Node to serwer przeznaczony do optymalizacji wykorzystania różnych zasobów (takich jak pojemność firmowego magazynu, przepustowości sieci i obciążenia procesorów w komputerach zarządzanych) wymaganych do ochrony danych przedsiębiorstwa. Cel ten jest osiągany dzięki organizowaniu lokalizacji służących jako dedykowane magazyny dla archiwów kopii zapasowych przedsiębiorstwa (skarbce zarządzane) i zarządzaniu nimi.

Węzły magazynowania umożliwiają tworzenie wysoce skalowalnej i elastycznej (pod względem obsługi sprzętu) infrastruktury magazynu. Skonfigurować można maksymalnie 20 węzłów magazynowania, a każdy z nich może zarządzać maksymalnie 20 skarbcami. Administrator obsługuje węzły magazynowania centralnie przy użyciu serwera zarządzania Acronis Backup & Recovery 10 Management Server (s. 427). Bezpośrednie połączenie konsoli z węzłem magazynowania nie jest możliwe.

Konfigurowanie infrastruktury magazynu

Należy zainstalować węzły magazynowania, dodać je do serwera zarządzania (procedura przypomina rejestrację (s. 427) komputera zarządzanego) i utworzyć skarbce centralne (s. 428). Podczas tworzenia skarbca centralnego należy określić jego ścieżkę, węzeł magazynowania do zarządzania tym skarbcem oraz operacje zarządzania, które będą wykonywane w skarbcu.

Skarbiec zarządzany można zorganizować:

- na lokalnych dyskach twardych węzła magazynowania;
- w udziale sieciowym;
- w sieci SAN (Storage Area Network);
- w magazynie NAS (Network Attached Storage);
- w bibliotece taśmowej dołączonej lokalnie do węzła magazynowania.

Wyróżnia się następujące operacje zarządzania.

Czyszczenie i sprawdzanie poprawności po stronie węzła magazynowania

Archiwa przechowywane w skarbcach niezarządzanych są obsługiwane przez agentów (s. 418) tworzących archiwa. Oznacza to, że zadaniem każdego agenta nie jest wyłącznie tworzenie kopii zapasowej danych w archiwum, ale również wykonywanie zadań związanych z obsługą archiwum oraz stosowanie reguł przechowywania i sprawdzania poprawności określonych w planie tworzenia kopii zapasowych (s. 425). Aby zmniejszyć niepotrzebne obciążenie procesora na komputerach zarządzanych, wykonywanie zadań związanych z obsługą można oddelegować do węzła magazynowania. Harmonogram zadań istnieje na komputerze, na którym znajduje się agent, i dlatego korzysta z zegara i zdarzeń komputera. Agent musi zainicjować czyszczenie po stronie węzła magazynowania (s. 420) i sprawdzanie poprawności po stronie węzła magazynowania (s. 429) zgodnie z harmonogramem. Aby było to możliwe, agent musi działać w trybie online. Dalsze czynności są wykonywane w węźle magazynowania.

Tej funkcji nie można wyłączyć w skarbcu zarządzanym. Następne dwie operacje są opcjonalne.

Deduplikacja

Skarbiec zarządzany można skonfigurować jako skarbiec deduplikacji. Oznacza to, że identyczne dane zostaną uwzględnione w kopii zapasowej tylko raz, aby zminimalizować wykorzystanie sieci podczas tworzenia kopii zapasowej oraz zmniejszyć ilość zajmowanego miejsca w archiwum. Aby uzyskać więcej informacji na ten temat, zobacz sekcję „Deduplikacja (s. 81)” w Podręczniku użytkownika.

Szyfrowanie

Skarbiec zarządzany można skonfigurować, tak aby wszystkie zapisywane w nim dane były szyfrowane, a wszystkie odczytywane dane — deszyfrowane w czasie rzeczywistym przez węzeł magazynowania przy użyciu klucza szyfrującego skarbca, który będzie przechowywany na serwerze węzłów. W przypadku kradzieży nośnika magazynu lub uzyskania do niego dostępu przez osobę nieautoryzowaną odszyfrowanie zawartości skarbca bez dostępu do wspomnianego węzła magazynowania będzie niemożliwe.

Jeśli archiwum jest już zaszyfrowane przez agenta, szyfrowanie po stronie węzła magazynowania zostanie zastosowane po szyfrowaniu wykonanym przez agenta.

PXE Server

Serwer Acronis PXE Server umożliwia uruchamianie komputerów na komponentach startowych Acronis za pośrednictwem sieci.

Uruchomienie przez sieć:

- eliminuje potrzebę lokalnej obecności technika w celu zainstalowania nośnika startowego (s. 424) w systemie, który ma zostać uruchomiony;
- w czasie operacji grupowych skraca czas potrzebny do uruchomienia wielu komputerów (w porównaniu z korzystaniem z fizycznego nośnika startowego).

Serwer licencji

Serwer umożliwiający zarządzanie licencjami produktów Acronis i instalowanie komponentów wymagających licencji.

Aby uzyskać więcej informacji na temat serwera licencji Acronis License Server, zobacz sekcję „Korzystanie z serwera licencji Acronis License Server”.

1.3.5 Konsola zarządzania

Konsola zarządzania Acronis Backup & Recovery 10 Management Console to narzędzie administracyjne umożliwiające zdalny lub lokalny dostęp do agentów Acronis Backup & Recovery 10, a w wersjach produktu z funkcją zarządzania scentralizowanego — do serwera zarządzania Acronis Backup & Recovery 10 Management Server.

Konsola jest dystrybuowana w dwóch wersjach: dla systemu Windows i systemu Linux. Mimo że obie wersje umożliwiają łączenie się z dowolnym agentem Acronis Backup & Recovery 10 i serwerem zarządzania Acronis Backup & Recovery 10 Management Server, zalecane jest korzystanie z konsoli dla systemu Windows (o ile wybór jest możliwy). Konsola instalowana w systemie Linux ma ograniczoną funkcjonalność:

- zdalna instalacja komponentów Acronis Backup & Recovery 10 jest niedostępna;
- funkcje związane z usługą Active Directory, takie jak przeglądanie usługi AD, są niedostępne.

1.3.6 Generator nośnika startowego

Generator nośnika startowego Acronis to specjalne narzędzie do tworzenia nośnika startowego (s. 424). Istnieją dwie wersje generatora nośnika: dla systemów Windows i Linux.

Generator nośnika dla systemu Windows umożliwia tworzenie nośnika startowego na podstawie środowiska preinstalacyjnego systemu Windows lub jądra systemu Linux. Dodatek Universal Restore (s. 20) umożliwia tworzenie nośnika startowego, za pomocą którego można przywrócić dane na komputer o innej konfiguracji sprzętowej. Dodatek ten niweluje różnice między urządzeniami istotnymi dla uruchamiania systemu Windows, takimi jak kontrolery pamięci, płyta główna i chipset.

Generator nośnika dla systemu Linux umożliwia tworzenie nośnika startowego na podstawie jądra systemu Linux.

Dodatek Deduplication (s. 20) umożliwia tworzenie nośnika startowego, za pomocą którego można utworzyć kopię zapasową w skarbcu deduplikacji. Dodatek ten można zainstalować w obu wersjach generatora nośnika.

1.3.7 Program Acronis Wake-on-LAN Proxy

Program Acronis Wake-on-LAN Proxy włącza wybudzanie serwera zarządzania Acronis Backup & Recovery 10 Management Server w celu tworzenia kopii zapasowych komputerów znajdujących się w innej podsieci. Program Acronis Wake-on-LAN Proxy należy zainstalować na dowolnym serwerze w podsieci obejmującej komputery, których kopię zapasową chcesz utworzyć.

1.4 Obsługiwane systemy plików

Program Acronis Backup & Recovery 10 umożliwia tworzenie kopii zapasowych i odzyskiwanie następujących systemów plików z poniższymi ograniczeniami:

- FAT16/32
- NTFS
- Ext2/Ext3/Ext4
- ReiserFS3 — nie można odzyskiwać poszczególnych plików z kopii zapasowych dysków znajdujących się węźle magazynowania Acronis Backup & Recovery 10 Storage Node.

- ReiserFS4 — odzyskiwanie woluminu bez możliwości zmiany jego rozmiaru; nie można odzyskiwać poszczególnych plików z kopii zapasowych dysków znajdujących się w węźle magazynowania Acronis Backup & Recovery 10 Storage Node.
- XFS — odzyskiwanie woluminu bez możliwości zmiany jego rozmiaru; nie można odzyskiwać poszczególnych plików z kopii zapasowych dysków znajdujących się w węźle magazynowania Acronis Backup & Recovery 10 Storage Node.
- JFS — nie można odzyskiwać poszczególnych plików z kopii zapasowych dysków znajdujących się w węźle magazynowania Acronis Backup & Recovery 10 Storage Node.
- Plik wymiany (SWAP) systemu Linux.

Program Acronis Backup & Recovery 10 umożliwia tworzenie kopii zapasowych oraz odzyskiwanie uszkodzonych lub nieobsługiwanych systemów plików metodą „sektor po sektorze”.

1.5 Obsługiwane systemy operacyjne

Acronis License Server

- Windows XP Professional SP2 lub nowszy (x86, x64)
- Windows 2000 SP4 — wszystkie wersje z wyjątkiem Datacenter
- Windows Server 2003/2003 R2 — wersje Standard i Enterprise (x86, x64)
- Windows Small Business Server 2003/2003 R2 (x86)
- Windows Vista — wszystkie wersje z wyjątkiem Vista Home Basic i Vista Home Premium (x86, x64)
- Windows 7 SP1 — wszystkie wersje z wyjątkiem Starter i Home (x86, x64)
- Windows Server 2008 — wersje Standard i Enterprise (x86, x64)
- Windows Small Business Server 2008 (x64)
- Windows Small Business Server 2011
- Windows Server 2008 R2 SP1 — wersje Standard, Enterprise, Datacenter, Foundation
- Windows MultiPoint Server 2010

Acronis Backup & Recovery 10 Management Console

- Windows XP Professional SP2 lub nowszy (x86, x64)
- Windows 2000 SP4 — wszystkie wersje z wyjątkiem Datacenter
- Windows Server 2003/2003 R2 — wersje Standard i Enterprise (x86, x64)
- Windows Small Business Server 2003/2003 R2 (x86)
- Windows Vista — wszystkie wersje (x86, x64)
- Windows 7 SP1 — wszystkie wersje (x86, x64)
- Windows Server 2008 — wersje Standard i Enterprise (x86, x64)
- Windows Small Business Server 2008 (x64)
- Windows Small Business Server 2011
- Windows Server 2008 R2 SP1 — wersje Standard, Enterprise, Datacenter, Foundation
- Windows MultiPoint Server 2010

Acronis Backup & Recovery 10 Management Server i Acronis Backup & Recovery 10 Storage Node

- Windows XP Professional SP3 (x86, x64)

- Windows 2000 SP4 — wszystkie wersje z wyjątkiem Datacenter
- Windows Server 2003/2003 R2 — wersje Standard i Enterprise (x86, x64)
- Windows Small Business Server 2003/2003 R2 (x86)
- Windows Vista — wszystkie wersje z wyjątkiem Vista Home Basic i Vista Home Premium (x86, x64)
- Windows 7 SP1* — wszystkie wersje z wyjątkiem Starter i Home (x86, x64)
- Windows Server 2008 — wersje Standard i Enterprise (x86, x64)
- Windows Small Business Server 2008 (x64)
- Windows Small Business Server 2011
- Windows Server 2008 R2 SP1* — wersje Standard, Enterprise, Datacenter, Foundation
- Windows MultiPoint Server 2010*

* Program Acronis Backup & Recovery 10 Storage Node obsługuje biblioteki taśmowe i zmieniacze za pomocą systemu Zarządzanie magazynem wymiennym (RSM). Ponieważ system RSM nie jest obsługiwany w systemach operacyjnych Windows 7, Windows Server 2008 R2 i Windows MultiPoint Server 2010, zainstalowany w nich węzeł magazynu nie będzie obsługiwać bibliotek taśmowych i zmieniaczy.

Acronis Backup & Recovery 10 Agent dla ESX/ESXi

- VMware ESX Infrastructure 3.5 Update 2+
- VMware ESX/ESXi 4.0 i 4.1

Agent dla ESX/ESXi jest dostarczany jako urządzenie wirtualne.

Agent dla ESX/ESXi obsługuje wszystkie licencje VMware ESXi poza bezpłatną. Jest to spowodowane używaniem przez agenta urządzenia Remote Command Line, które w bezpłatnej wersji VMware ESXi ma ograniczenie tylko do odczytu. Agent działa w trakcie okresu próbnego programu VMware ESXi. Po wprowadzeniu bezpłatnego klucza seryjnego VMware ESXi agent ESX/ESXi przestanie działać.

Acronis Backup & Recovery 10 Agent dla Hyper-V

- Windows Server 2008/2008 R2 (x64) z Hyper-V
- Microsoft Hyper-V Server 2008/2008 R2

Ten agent instaluje hosta Hyper-V jako dodatek do komponentu Acronis Backup & Recovery 10 Agent dla systemu Windows.

Acronis Backup & Recovery 10 Agent dla systemu Windows

- Windows XP Professional SP2 lub nowszy (x86, x64)
- Windows 2000 SP4 — wszystkie wersje z wyjątkiem Datacenter
- Windows Server 2003/2003 R2 — wersje Standard i Enterprise (x86, x64)
- Windows Small Business Server 2003/2003 R2 (x86)
- Windows Vista — wszystkie wersje z wyjątkiem Vista Home Basic i Vista Home Premium (x86, x64)
- Windows 7 SP1 — wszystkie wersje z wyjątkiem Starter i Home (x86, x64)
- Windows Server 2008 — wersje Standard i Enterprise (x86, x64)
- Windows Small Business Server 2008 (x64)
- Windows Small Business Server 2011
- Windows Server 2008 R2 SP1 — wersje Standard, Enterprise, Datacenter, Foundation

- Windows MultiPoint Server 2010

Acronis Backup & Recovery 10 Agent dla systemu Linux

- System Linux z jądrem 2.4.20 lub nowszym (łącznie z jądrami 2.6.x) i biblioteką glibc 2.3.2 lub nowszą.
- Różne 32-bitowe i 64-bitowe dystrybucje systemu Linux, w tym:
  - Red Hat Enterprise Linux 4.x i 5.x
  - Red Hat Enterprise Linux 6
  - Ubuntu 9.04 (Jaunty Jackalope), 9.10 (Karmic Koala) i 10.04 (Lucid Lynx)
  - Fedora 11 i 12
  - SUSE Linux Enterprise Server 10 i 11
  - Debian 4 (Lenny) i 5 (Etch)
  - CentOS 5
- Agent dla systemu Linux jest 32-bitowym plikiem wykonywalnym. W celu uwierzytelniania agent wykorzystuje biblioteki systemowe, których 32-bitowe wersje nie zawsze są instalowane domyślnie w dystrybucjach 64-bitowych. W przypadku korzystania z agenta w 64-bitowej dystrybucji opartej na systemie RedHat (takiej jak RHEL, CentOS, Fedora) lub 64-bitowej dystrybucji SUSE, należy się upewnić, że w systemie są zainstalowane następujące pakiety 32-bitowe:

  pam.i386

  libselinux.i386

  libsepol.i386

  Pakiety te powinny być dostępne w repozytorium dystrybucji systemu Linux.
- Przed zainstalowaniem produktu w systemie, który nie używa menedżera pakietów RPM, takim jak Ubuntu, należy ręcznie zainstalować menedżer pakietów RPM, na przykład przy użyciu następującego polecenia (jako użytkownik root):

```
apt-get install rpm
```

Programy firmy Acronis nie obsługują systemów z interfejsem Extensible Firmware Interface (EFI). Co prawda partycję GPT można przywrócić za pomocą programu firmy Acronis, jeśli jest na niej zainstalowany system Windows, ale przywróconego systemu nie będzie można uruchomić. Program Acronis Backup & Recovery 10 umożliwia tworzenie kopii zapasowych i odzyskiwanie systemów operacyjnych zainstalowanych w trybie BIOS/MBR, nawet jeśli działają na serwerach obsługujących interfejs EFI. W przypadku większości serwerów ustawienia systemu BIOS umożliwiają uruchomienie instalacyjnego dysku CD w trybie BIOS/MBR zamiast w trybie EFI. W trybie MBR po zakończeniu instalacji dysk startowy zostaje podzielony na partycje przy użyciu standardu MBR, a nie GPT.

1.6 Wymagania systemowe

Komponenty instalowane w systemie operacyjnym

Komponent	Pamięć (oprócz systemu operacyjnego i uruchomionych aplikacji)	Miejsce na dysku wymagane podczas instalacji lub aktualizacji	Miejsce na dysku zajmowane przez komponenty	Dodatkowo
Komponenty instalowane w systemie Windows				
Pełna instalacja	300 MB	2,7 GB	1,7 GB wraz z serwerem SQL Express Server	
Agent dla systemu Windows	120 MB	700 MB	260 MB	
Agent dla Hyper-V (dodatek)	Zobacz „Agent dla systemu Windows”	50 MB	20 MB	
Generator nośnika startowego	80 MB	700 MB	300 MB	Napęd CD-RW lub DVD-RW
Management Console	30 MB	950 MB	450 MB	Rozdzielczość ekranu 1024*768 pikseli lub wyższa
Management Server	40 MB	250 MB 400 MB dla serwera SQL Express Server	250 MB 400 MB dla serwera SQL Express Server	
Wake-On-LAN Proxy	Minimalna	30 MB	5 MB	
Storage Node	100 MB	150 MB	150 MB W przypadku używania biblioteki taśm miejsce wymagane na bazę danych taśm: około 1 MB na każde 10 archiwów	Zalecane wymagania sprzętowe: 4 GB RAM Szybka pamięć masowa, taka ja sprzętowa macierz RAID
License Server	Minimalna	25 MB	25 MB	
PXE Server	5 MB	80 MB	15 MB	
Komponenty instalowane w systemie Linux				
Pełna instalacja	160 MB	400 MB	250 MB	
Agent dla systemu Linux	65 MB	150 MB	70 MB	

Generator nośnika startowego	70 MB	240 MB	140 MB	
Management Console	25 MB	100 MB	40 MB	
Komponenty instalowane na serwerze VMware ESX(i)				
Agent urządzenia ESX/ESXi Virtual Appliance	512 MB (ustawienie pamięci urządzenia wirtualnego)	5 GB	5 GB	Rezerwacja procesora: zalecane co najmniej 300 MHz W klastrze vCenter wymagane jest użycie magazynu współużytkowanego

Karta sieciowa lub wirtualna karta sieciowa jest wspólnym wymaganiem dla wszystkich komponentów.

Nośnik startowy

Typ nośnika	Pamięć	Rozmiar obrazu ISO	Dodatkowo
Oparty na środowisku Windows PE	512 MB	300 MB	
Oparty na systemie Linux	256 MB	130 MB	

1.7 Pomoc techniczna

Program pomocy technicznej i konserwacji

Jeśli będziesz potrzebować pomocy dotyczącej posiadanego produktu Acronis, przejdź na stronę http://www.acronis.pl/support/.

Aktualizacje produktów

Aby móc na bieżąco pobierać z naszej witryny internetowej najnowsze aktualizacje do wszystkich posiadanych produktów Acronis, zaloguj się na swoim koncie (http://www.acronis.pl/my) i zarejestruj produkty. Zobacz **Rejestrowanie produktów Acronis w witrynie internetowej** (http://kb.acronis.com/content/4834) i **Podręcznik użytkownika witryny internetowej firmy Acronis** (http://kb.acronis.com/content/8128). Artykuły dostępne są w języku angielskim.

2 Opis programu Acronis Backup & Recovery 10

W tej sekcji podjęto próbę przystępnego opisania programu, aby umożliwić czytelnikom korzystanie z niego w różnych okolicznościach bez konieczności odwoływania się do szczegółowych instrukcji.

2.1 Podstawowe pojęcia

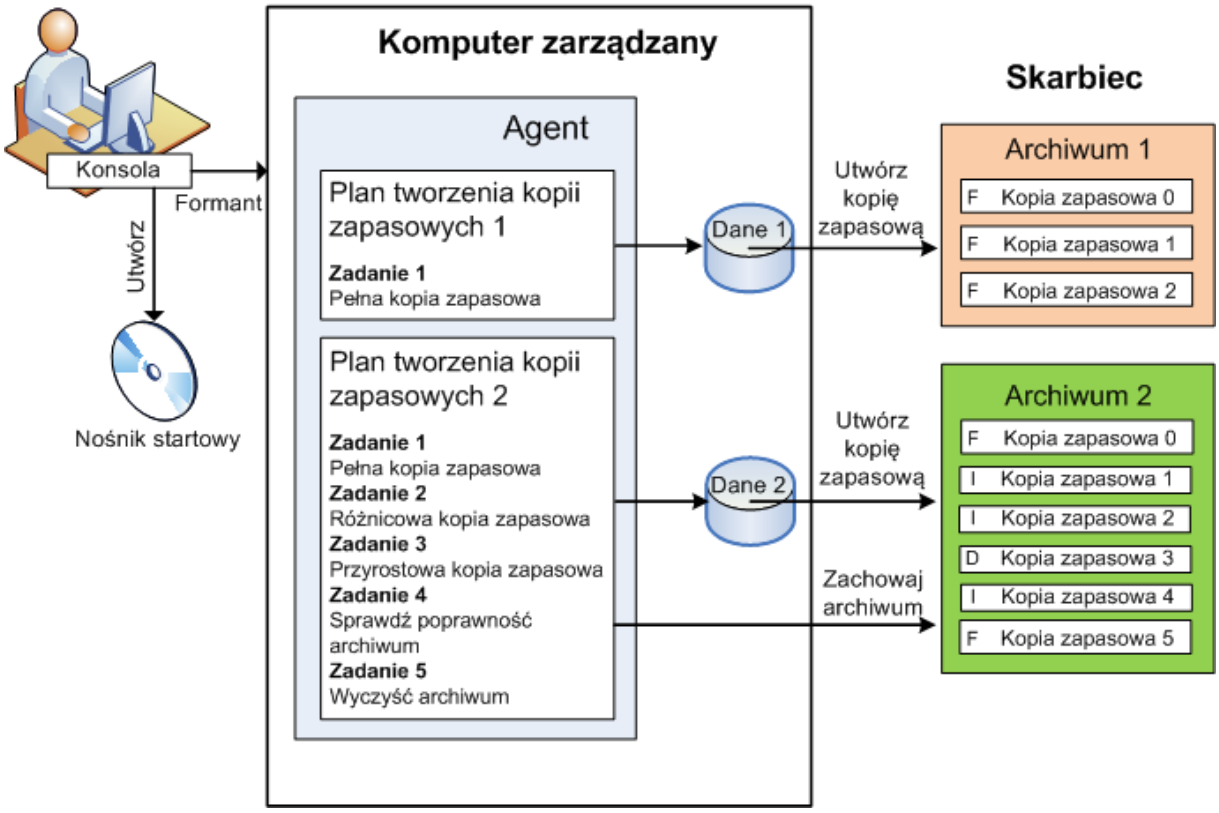
W tej sekcji można zapoznać się z podstawowymi pojęciami używanymi w graficznym interfejsie użytkownika i dokumentacji programu Acronis Backup & Recovery 10. Użytkowników zaawansowanych zachęcamy do skorzystania z tej sekcji jako instrukcji szybkiego rozpoczęcia pracy. Szczegółowe informacje można znaleźć w pomocy kontekstowej.

Tworzenie kopii zapasowych w systemie operacyjnym

1. W celu ochrony danych zainstaluj agenta (s. 418) Acronis Backup & Recovery 10 na komputerze, który od tego momentu stanie się komputerem zarządzanym (s. 423).
2. Aby umożliwić zarządzanie komputerem przy użyciu graficznego interfejsu użytkownika, zainstaluj konsolę Acronis Backup & Recovery 10 Management Console (s. 423) na tym samym komputerze lub na dowolnym komputerze, którego chcesz używać. W przypadku produktu w wersji autonomicznej pomiń ten krok, ponieważ konsola jest instalowana razem z agentem.
3. Uruchom konsolę. Aby umożliwić odzyskiwanie systemu operacyjnego komputera, jeśli jego uruchamianie kończy się niepowodzeniem, utwórz nośnik startowy (s. 424).
4. Podłącz konsolę do komputera zarządzanego.
5. Utwórz plan tworzenia kopii zapasowych (s. 425).

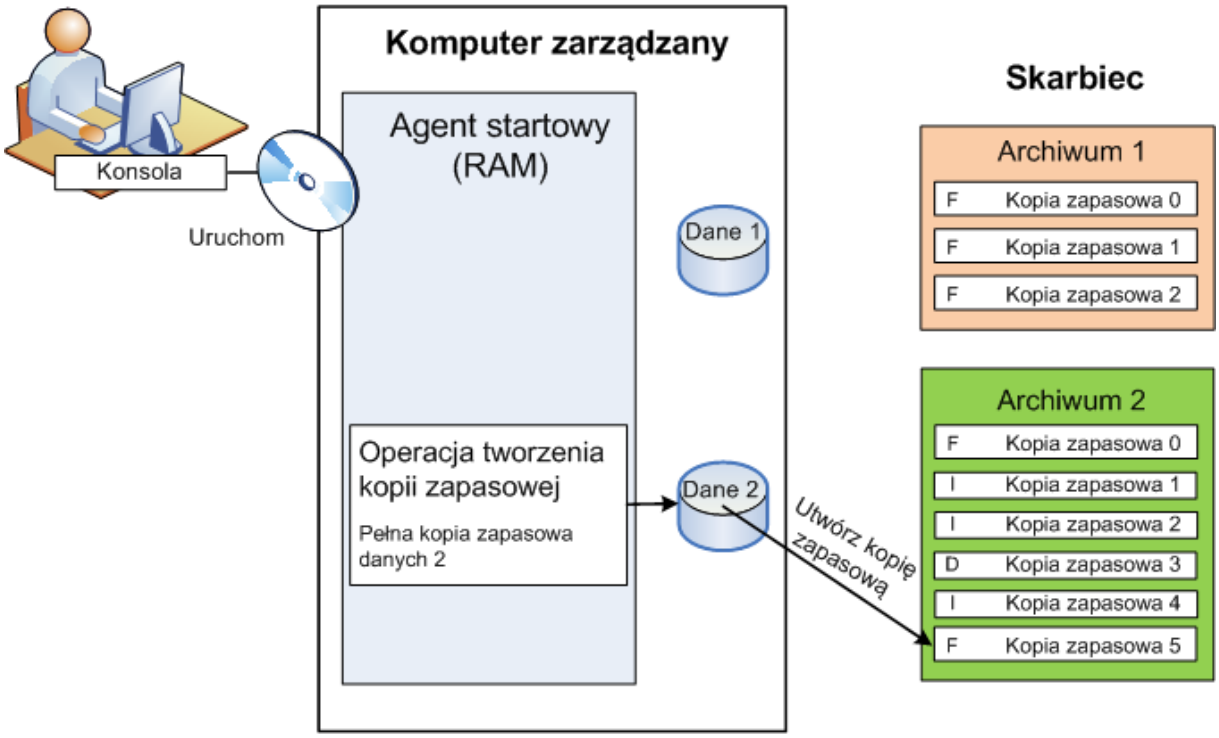
   W tym celu musisz określić przynajmniej dane, które mają być chronione, i lokalizację, w której będzie przechowywane archiwum kopii zapasowych (s. 419). W wyniku tego zostanie utworzony minimalny plan tworzenia kopii zapasowych składający się z jednego zadania (s. 431). Za każdym razem po ręcznym uruchomieniu zadania zostanie utworzona pełna kopia zapasowa (s. 424). Złożony plan tworzenia kopii zapasowych może składać się z wielu zadań uruchamianych zgodnie z harmonogramem oraz obejmować tworzenie pełnych, przyrostowych lub różnicowych kopii zapasowych (s. 36), wykonywanie operacji utrzymywania archiwów, takich jak sprawdzanie poprawności (s. 429) kopii zapasowych lub usuwanie przestarzałych kopii zapasowych (czyszczenie (s. 419) archiwów). Operacje tworzenia kopii zapasowych można dostosowywać przy użyciu różnych opcji tworzenia kopii zapasowych, takich jak opcje poleceń przed/po utworzeniu kopii zapasowej, dławienia przepustowości sieci, obsługi błędów lub powiadomień.
6. Na stronie **Plany i zadania tworzenia kopii zapasowych** można wyświetlać informacje o planach i zadaniach tworzenia kopii zapasowych oraz monitorować ich wykonywanie. Na stronie **Dziennik** można przeglądać dziennik operacji.
7. Lokalizacja, w której są przechowywane archiwa kopii zapasowych, nosi nazwę skarbca (s. 428). Przejdź do strony **Skarbce**, aby wyświetlić informacje o skarbcach. Przejdź dalej do określonego skarbca, aby wyświetlić archiwa i kopie zapasowe oraz ręcznie wykonać związane z nimi operacje (montowanie, sprawdzanie poprawności, usuwanie, wyświetlanie zawartości). Możesz również wybrać kopię zapasową, aby odzyskać z niej dane.

Poniższy diagram ilustruje opisane powyżej pojęcia. Więcej definicji można znaleźć w Słowniku.



Tworzenie kopii zapasowych przy użyciu nośnika startowego

Użytkownik może uruchomić komputer przy użyciu nośnika startowego, skonfigurować operację tworzenia kopii zapasowych w taki sam sposób jak prosty plan tworzenia kopii zapasowych oraz wykonać operację. Ułatwi to wyodrębnienie plików i woluminów logicznych z systemu, którego uruchamianie zakończyło się niepowodzeniem, pobranie obrazu z systemu offline lub utworzenie kopii zapasowej „sektor po sektorze” nieobsługiwanego systemu plików.



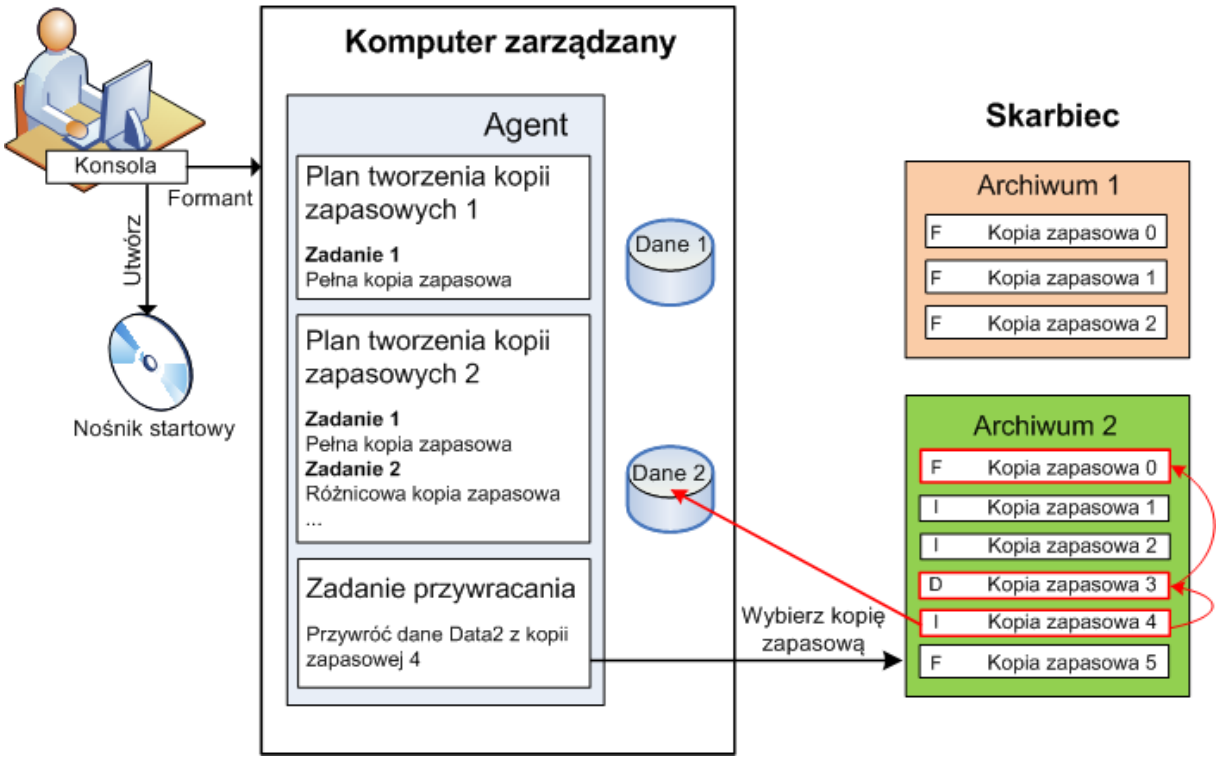
Odzyskiwanie w systemie operacyjnym

Gdy trzeba odzyskać dane, użytkownik tworzy zadanie odzyskiwania na komputerze zarządzanym. Określa magazyn, wybiera archiwum, a następnie wybiera kopię zapasową na podstawie daty i godziny utworzenia kopii zapasowej, a dokładniej — godziny rozpoczęcia tworzenia. W większości przypadków dane zostaną przywrócone do stanu z tego momentu.

Przykłady wyjątków od tej reguły:
Odzyskiwanie bazy danych z kopii zapasowej zawierającej dziennik transakcji (pojedyncza kopia zapasowa zawiera wiele punktów odzyskiwania, dzięki czemu można dokonywać dodatkowych wyborów).
Odzyskiwanie wielu plików z kopii zapasowej plików utworzonej bez migawki (każdy plik zostanie przywrócony do stanu z momentu, w którym został faktycznie skopiowany do kopii zapasowej).

Użytkownik określa także miejsce docelowe, do którego mają być odzyskiwane dane. Operację odzyskiwania można dostosowywać przy użyciu opcji odzyskiwania, takich jak opcje poleceń przed/po odzyskaniu, obsługi błędów lub powiadomień.

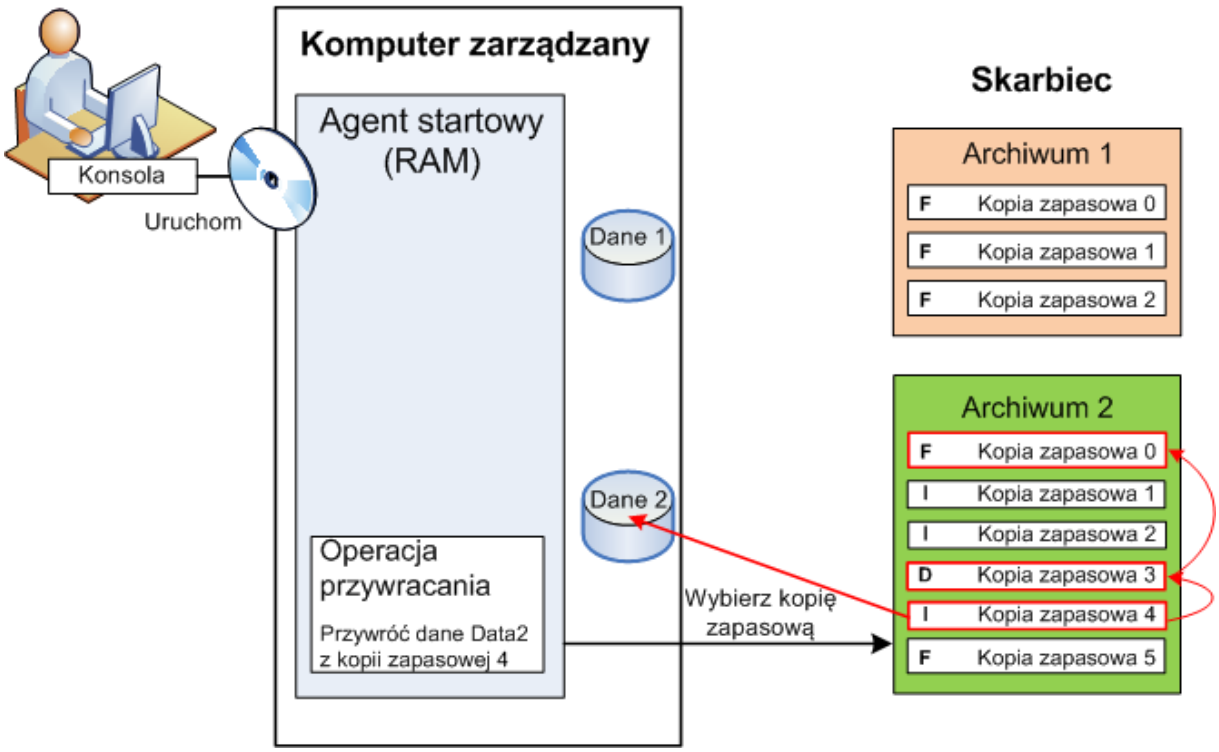
Poniższy diagram ilustruje odzyskiwanie danych w systemie operacyjnym (online). W czasie wykonywania operacji odzyskiwania na komputerze nie może być tworzona żadna kopia zapasowa. W razie potrzeby można podłączyć konsolę do innego komputera i skonfigurować operację odzyskiwania na tym komputerze. Taka możliwość (zdalne odzyskiwanie równoległe) pojawiła się po raz pierwszy w programie Acronis Backup & Recovery 10. Starsze produkty Acronis nie mają tej funkcji.



Odzyskiwanie przy użyciu nośnika startowego

Odzyskiwanie na woluminie zablokowanym przez system operacyjny, na przykład na woluminie, na którym znajduje się system operacyjny, wymaga ponownego uruchomienia do środowiska startowego będącego częścią agenta. Po zakończeniu odzyskiwania odzyskany system operacyjny automatycznie przechodzi w tryb online.

Jeśli uruchamianie komputera kończy się niepowodzeniem lub trzeba odzyskać dane do systemu odzyskanego po awarii, należy uruchomić komputer przy użyciu nośnika startowego i skonfigurować operację odzyskiwania w taki sam sposób jak zadanie odzyskiwania. Poniższy diagram ilustruje odzyskiwanie przy użyciu nośnika startowego.



2.2 Uprawnienia użytkownika na zarządzanym komputerze

Windows

Podczas zarządzania komputerem z systemem Windows zakres uprawnień użytkownika związanych z zarządzaniem zależy od jego uprawnień na komputerze.

Zwykli użytkownicy

Zwykły użytkownik, np. należący do grupy Użytkownicy, ma następujące uprawnienia do zarządzania:

- Tworzenie kopii zapasowych na poziomie plików i odzyskiwanie plików, do których użytkownik ma prawa dostępu — ale bez używania migawek na poziomie plików.
- Tworzenie planów i zadań tworzenia kopii zapasowych i zarządzanie nimi.
- Wyświetlanie, ale bez możliwości zarządzania, planów i zadań tworzenia kopii zapasowych utworzonych przez innych użytkowników.
- Wyświetlanie lokalnego dziennika zdarzeń.

Administratorzy

Użytkownik z uprawnieniami administratora, np. należący do grupy Administratorzy lub Operatorzy kopii zapasowych, mają następujące dodatkowe uprawnienia do zarządzania:

- Tworzenie i odzyskiwanie całego komputera lub dowolnych znajdujących się na nim danych, w tym również z użyciem migawek dysków.

Użytkownicy należący do grupy Administratorzy mogą również:

- Wyświetlać plany i zadania tworzenia kopii zapasowych utworzone przez użytkowników na danym komputerze i zarządzać nimi.

Linux

Podczas zarządzania komputerem z systemem Linux użytkownik uzyskuje uprawnienia użytkownika root i może:

- Tworzyć kopie zapasowe i odzyskiwać dane lub cały komputer, mając pełną kontrolę nad wszystkimi działaniami agenta Acronis Backup & Recovery 10 oraz dostęp do plików dzienników na komputerze.
- Zarządzać lokalnymi planami i zadaniami tworzenia kopii zapasowych należącymi do dowolnego użytkownika zarejestrowanego w systemie operacyjnym.

Aby uniknąć rutynowego logowania się w systemie jako użytkownik root, można zalogować się jako zwykły użytkownik, a następnie przełączać użytkowników w razie konieczności.

2.3 Właściciele i poświadczenia

W tej sekcji wyjaśniono pojęcie właściciela oraz znaczenie poświadczeń planu (lub zadania) tworzenia kopii zapasowych.

Właściciel planu (zadania)

Właścicielem lokalnego planu tworzenia kopii zapasowych jest użytkownik, który utworzył lub jako ostatni zmodyfikował ten plan.

Właścicielem scentralizowanego planu tworzenia kopii zapasowych jest administrator serwera zarządzania, który utworzył lub jako ostatni zmodyfikował scentralizowane zasady duplikujące ten plan.

Właścicielem zadań należących do planu tworzenia kopii zapasowych (lokalnego lub scentralizowanego) jest właściciel tego planu.

Właścicielem zadań nienależących do planu tworzenia kopii zapasowych, takich jak zadanie odzyskiwania, jest użytkownik, który utworzył lub jako ostatni zmodyfikował zadanie.

Zarządzanie planem (zadaniem), którego właścicielem jest inny użytkownik

Użytkownik z uprawnieniami administratora na komputerze może modyfikować zadania i lokalne plany tworzenia kopii zapasowych, których właścicielem jest dowolny użytkownik zarejestrowany w systemie operacyjnym.

Otwarcie do edycji planu lub zadania, którego właścicielem jest inny użytkownik, powoduje wyczyszczenie wszystkich haseł ustawionych w zadaniu. To zapobiega stosowaniu sztuczki polegającej na zmodyfikowaniu ustawień i pozostawieniu haseł. Przy każdej próbie edycji planu

(zadania) zmodyfikowanego ostatnio przez innego użytkownika program wyświetla ostrzeżenie. Po wyświetleniu ostrzeżenia dostępne są dwie opcje:

- Kliknij **Anuluj** i utwórz własny plan lub zadanie. Oryginalne zadanie pozostanie nienaruszone.
- Kontynuuj edycję. Trzeba będzie wprowadzić wszystkie poświadczenia wymagane do wykonania planu lub zadania.

Właściciel archiwum

Właścicielem archiwum jest użytkownik, który zapisał je w miejscu docelowym. Dokładniej — jest to użytkownik, którego konto zostało określone podczas tworzenia planu tworzenia kopii zapasowych w kroku **Miejsce docelowe kopii zapasowej**. Domyślnie są używane poświadczenia planu.

Poświadczenia planu i poświadczenia zadania

Dowolne zadanie jest uruchamiane na komputerze w imieniu użytkownika. Podczas tworzenia planu lub zadania dostępna jest opcja jawnego określenia konta, na którym będzie uruchamiany plan lub zadanie. Wybór zależy od tego, czy plan lub zadanie mają być uruchamiane ręcznie, czy też zgodnie z harmonogramem.

Uruchamianie ręczne

Krok **Poświadczenia planu (zadania)** można pominąć. Zadanie za każdym razem będzie uruchamiane z poświadczeniami, z którymi aktualnie jest zalogowany użytkownik. Zadanie może zostać uruchomione przez dowolną osobę mającą uprawnienia administracyjne na danym komputerze. Zostanie ono uruchomione z poświadczeniami tej osoby.

Jeśli poświadczenia zadania zostaną określone jawnie, zadanie będzie uruchamiane zawsze z tymi samymi poświadczeniami, niezależnie od tego, który użytkownik faktycznie uruchamia zadanie. Aby określić poświadczenia zadania, na stronie tworzenia planu (zadania):

1. Zaznacz pole wyboru **Widok zaawansowany**.
2. Wybierz **Ogólne -> Poświadczenia planu (zadania) -> Zmień**.
3. Wprowadź poświadczenia, z którymi będzie uruchamiany plan (zadanie).

Uruchamianie zaplanowane lub opóźnione

Poświadczenia planu (zadania) są obowiązkowe. Pominięcie kroku dotyczącego poświadczeń spowoduje, że po zakończeniu tworzenia planu (zadania) zostanie wyświetlony monit o podanie poświadczeń.

Dlaczego program zmusza do określenia poświadczeń?

Zaplanowane lub opóźnione zadanie musi zostać uruchomione niezależnie od tego, czy jest zalogowany jakikolwiek użytkownik (na przykład podczas wyświetlania ekranu powitalnego systemu Windows), czy też jest zalogowany użytkownik inny niż właściciel zadania. Wystarczy, że o zaplanowanej godzinie rozpoczęcia zadania komputer będzie włączony (tzn. nie będzie w trybie wstrzymania ani hibernacji). Dlatego harmonogram Acronis wymaga jawnego określenia poświadczeń, aby mógł uruchamiać zadanie.

2.4 Pełne, przyrostowe i różnicowe kopie zapasowe

Program Acronis Backup & Recovery 10 umożliwia korzystanie z popularnych schematów tworzenia kopii zapasowych, takich jak Dziadek-ojciec-syn i Wieża Hanoi, a także tworzenie niestandardowych schematów tworzenia kopii zapasowych. Wszystkie schematy tworzenia kopii zapasowych są oparte

na metodach tworzenia pełnych, przyrostowych i różnicowych kopii zapasowych. Termin „schemat" tak naprawdę oznacza algorytm stosowania tych metod oraz algorytm czyszczenia archiwum.

Porównywanie ze sobą metod tworzenia kopii zapasowych nie ma większego sensu, ponieważ w schemacie tworzenia kopii zapasowych działają one zespołowo. Każda metoda powinna pełnić określoną rolę, w zależności od jej zalet. Profesjonalny schemat tworzenia kopii zapasowych wykorzystuje zalety wszystkich metod tworzenia kopii zapasowych, ograniczając wpływ wszystkich wad tych metod. Na przykład cotygodniowa różnicowa kopia zapasowa zawiera czyszczenie archiwum, ponieważ może zostać łatwo usunięta wraz z cotygodniowym zestawem zależnych od niej codziennych przyrostowych kopii zapasowych.

Proces tworzenia kopii zapasowej metodą pełną, przyrostową lub różnicową powoduje utworzenie kopii zapasowej (s. 424) odpowiedniego typu.

Pełna kopia zapasowa

Pełna kopia zapasowa przechowuje wszystkie dane wybrane do utworzenia kopii zapasowej. Pełna kopia zapasowa stanowi podstawę każdego archiwum i tworzy podwaliny pod przyrostowe oraz różnicowe kopie zapasowe. Archiwum może zawierać wiele pełnych kopii zapasowych lub składać się wyłącznie z pełnych kopii zapasowych. Pełna kopia zapasowa jest samowystarczalna — odzyskanie danych z pełnej kopii zapasowej nie wymaga dostępu do żadnej innej kopii zapasowej.

Powszechnie akceptowany jest fakt, że wykonanie pełnej kopii zapasowej trwa najdłużej, ale jej przywrócenie jest najszybsze. Dzięki technologiom firmy Acronis odzyskiwanie z przyrostowej kopii zapasowej nie musi być wolniejsze niż odzyskiwanie z kopii pełnej.

Pełna kopia zapasowa jest najbardziej przydatna, gdy:

- trzeba przywrócić system do stanu początkowego;
- stan początkowy nie zmienia się często, dzięki czemu nie trzeba regularnie tworzyć kopii zapasowych.

Przykład: Kawiarenka internetowa, szkoła lub laboratorium uniwersyteckie, gdzie administrator często cofa zmiany wprowadzone przez uczniów/studentów lub klientów, natomiast rzadko aktualizuje referencyjną kopię zapasową (tak naprawdę tylko po zainstalowaniu aktualizacji oprogramowania). W takim przypadku czas tworzenia kopii zapasowej nie ma większego znaczenia, a czas odzyskiwania systemów z pełnej kopii zapasowej będzie minimalny. W celu zapewnienia większej niezawodności administrator może mieć kilka egzemplarzy kopii zapasowej.

Przyrostowa kopia zapasowa

Przyrostowa kopia zapasowa przechowuje zmiany danych w porównaniu do **ostatniej kopii zapasowej**. Odzyskanie danych z przyrostowej kopii zapasowej wymaga dostępu do innych kopii zapasowych z tego samego archiwum.

Przyrostowa kopia zapasowa jest najbardziej przydatna, gdy:

- trzeba zachować możliwość przywracania dowolnego z wielu zapisanych stanów,
- zmiany danych są raczej niewielkie w porównaniu z całkowitym rozmiarem danych.

Powszechnie akceptowany jest fakt, że przyrostowe kopie zapasowe są mniej niezawodne niż kopie pełne, ponieważ uszkodzenie jednej kopii zapasowej w „łańcuchu" powoduje, że nie można więcej używać następnych kopii. Jednak gdy potrzebnych jest wiele wcześniejszych wersji danych, przechowywanie wielu pełnych kopii zapasowych nie jest dobrym rozwiązaniem, ponieważ niezawodność zbyt dużego archiwum jest jeszcze bardziej wątpliwa.

Przykład: Tworzenie kopii zapasowej dziennika transakcji bazy danych.

Różnicowa kopia zapasowa

Różnicowa kopia zapasowa przechowuje zmiany danych w porównaniu do **najnowszej pełnej kopii zapasowej**. Odzyskanie danych z różnicowej kopii zapasowej wymaga dostępu do odpowiedniej pełnej kopii zapasowej. Różnicowa kopia zapasowa jest najbardziej przydatna, gdy:

- użytkownik jest zainteresowany zapisywaniem wyłącznie najnowszego stanu danych,
- zmiany danych są raczej niewielkie w porównaniu z całkowitym rozmiarem danych.

Typowy wniosek jest następujący: „tworzenie różnicowych kopii zapasowych trwa dłużej, a ich przywracanie krócej, natomiast tworzenie kopii przyrostowych jest szybsze, a ich przywracanie trwa dłużej". Tak naprawdę nie ma fizycznej różnicy między przyrostową kopią zapasową dołączoną do pełnej kopii zapasowej a różnicową kopią zapasową dołączoną do tej samej pełnej kopii zapasowej w tym samym punkcie w czasie. Wspomniana powyżej różnica zakłada utworzenie różnicowej kopii zapasowej po (lub zamiast) utworzeniu wielu przyrostowych kopii zapasowych.

Przyrostowa lub różnicowa kopia zapasowa utworzona po defragmentacji dysku może być znacznie większa niż zwykle, ponieważ defragmentacja powoduje zmianę lokalizacji plików na dysku, a kopia zapasowa odzwierciedla te zmiany. Po defragmentacji dysku zaleca się ponowne utworzenie pełnej kopii zapasowej.

W poniższej tabeli podsumowano zalety i wady poszczególnych typów kopii zapasowych w oparciu o popularną wiedzę na ich temat. W rzeczywistości te parametry zależą od wielu czynników, między innymi ilości, szybkości i wzorca zmian danych, natury danych, specyfikacji fizycznych urządzeń, ustawionych opcji tworzenia kopii zapasowych/odzyskiwania. Najlepszą pomocą przy wybieraniu optymalnego schematu tworzenia kopii zapasowych jest doświadczenie.

Parametr	Pełna kopia zapasowa	Różnicowa kopia zapasowa	Przyrostowa kopia zapasowa
Miejsce do przechowywania	Maksymalne	Średnie	Minimalne
Czas tworzenia	Maksymalny	Średni	Minimalny
Czas odzyskiwania	Minimalny	Średni	Maksymalny

2.5 Schemat tworzenia kopii zapasowych GFS

W tej sekcji omówiono implementację schematu tworzenia kopii zapasowych Dziadek-ojciec-syn (GFS) w programie Acronis Backup & Recovery 10.

Ten schemat tworzenia kopii zapasowych nie pozwala na tworzenie kopii zapasowych częściej niż raz dziennie. Schemat umożliwia oznaczanie dziennych, tygodniowych i miesięcznych cykli w harmonogramie tworzenia dziennych kopii zapasowych oraz ustawianie okresów przechowywania dziennych, miesięcznych i tygodniowych kopii zapasowych. Dzienne kopie zapasowe są nazywane „synami", tygodniowe — „ojcami", a najtrwalsze, miesięczne kopie zapasowe noszą nazwę „dziadków".

GFS jako schemat rotacji taśm

Początkowo schemat GFS powstał jako schemat rotacji taśm i często jest tak nazywany. Schematy rotacji taśm nie zapewniają automatyzacji. Określają jedynie:

- ile taśm potrzeba, aby umożliwić odzyskiwanie z żądaną rozdzielczością (przedział czasu między punktami odzyskiwania) i okresem wycofywania;
- które taśmy powinny zostać zastąpione podczas kolejnego tworzenia kopii zapasowej.

Schematy rotacji taśm umożliwiają tworzenie kopii zapasowych z wykorzystaniem minimalnej liczby kaset, aby nadmiar używanych taśm nie utrudniał pracy. Warianty schematu rotacji taśm GFS opisano

w licznych źródłach internetowych. Podczas tworzenia kopii zapasowych na podłączonym lokalnie urządzeniu taśmowym można używać dowolnego z tych wariantów.

Schemat GFS w programach Acronis

Program Acronis Backup & Recovery 10 umożliwia łatwe skonfigurowanie planu tworzenia kopii zapasowych, który będzie regularnie tworzył kopie zapasowe danych i czyścił archiwum wynikowe zgodnie ze schematem GFS.

Plan tworzenia kopii zapasowych należy utworzyć w zwykły sposób. Jako miejsce docelowe kopii zapasowych należy wybrać dowolne urządzenie pamięci umożliwiające przeprowadzanie automatycznego czyszczenia, na przykład urządzenie pamięci z dyskiem twardym lub automatyczną bibliotekę taśm. (Ponieważ miejsca zwolnionego na taśmie w wyniku czyszczenia nie można wykorzystać ponownie, dopóki cała taśma nie będzie wolna, używając schematu GFS w bibliotece taśm (s. 164), należy wziąć pod uwagę dodatkowe kwestie).

Poniżej objaśniono ustawienia charakterystyczne dla schematu tworzenia kopii zapasowych GFS.

Ustawienia planu tworzenia kopii zapasowych związane ze schematem GFS

Rozpocznij tworzenie kopii zapasowej o:

Utwórz kopię zapasową dnia:

Ten krok powoduje utworzenie całkowitego harmonogramu tworzenia kopii zapasowych, tzn. zdefiniowanie wszystkich dni, kiedy muszą być tworzone kopie zapasowe.

Załóżmy, że wybrano tworzenie kopii zapasowych o godzinie 20.00 w dni robocze. Poniżej przedstawiono zdefiniowany przez użytkownika cały harmonogram.

„B” oznacza kopię zapasową (ang. „backup”).

Cały harmonogram.
Harmonogram: dni robocze o godz. 20.00

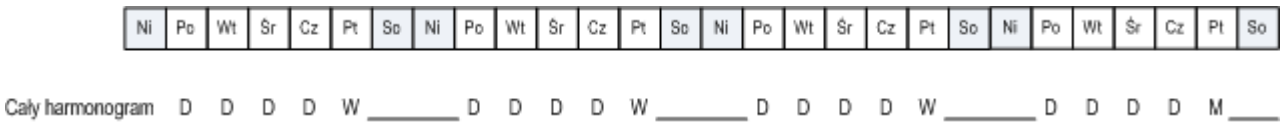
Co tydzień/Co miesiąc

Ten krok powoduje utworzenie dziennych, tygodniowych i miesięcznych cykli w harmonogramie.

Spośród dni wybranych w poprzednim kroku należy wybrać dzień tygodnia. Każda pierwsza, druga i trzecia kopia zapasowa utworzona w tym dniu tygodnia będzie uważana za tygodniową kopię zapasową. Każda czwarta kopia zapasowa utworzona w tym dniu tygodnia będzie uważana za miesięczną kopię zapasową. Kopie zapasowe tworzone w pozostałe dni będą uważane za dzienne kopie zapasowe.

Załóżmy, że jako dzień tworzenia tygodniowych/miesięcznych kopii zapasowych wybrano piątek. Poniżej przedstawiono cały harmonogram oznaczony zgodnie z wybraną opcją.

„D” oznacza kopię zapasową uważaną za dzienną. „W” oznacza kopię zapasową uważaną za tygodniową (ang. „weekly”). „M” oznacza kopię zapasową uważaną za miesięczną.

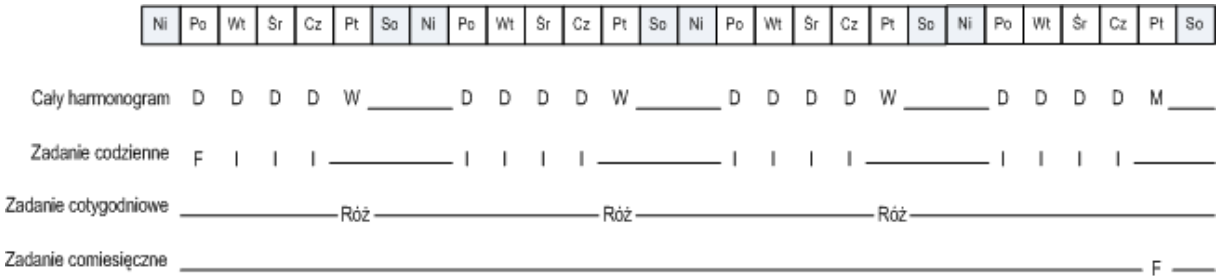


Harmonogram oznaczony zgodnie ze schematem GFS.
Harmonogram: dni robocze o godz. 20.00
Co tydzień/Co miesiąc: Piątek

Firma Acronis używa przyrostowych i różnicowych kopii zapasowych, które pomagają oszczędzać miejsce do przechowywania oraz optymalizują czyszczenie, dzięki czemu nie jest potrzebna konsolidacja. Z punktu widzenia metod tworzenia kopii zapasowych tygodniowa kopia zapasowa jest kopią różnicową (Dif, ang. „differential"), miesięczna kopia zapasowa jest kopią pełną (F, ang. „full"), a dzienna kopia zapasowa jest kopią przyrostową (I, ang. „incremental"). Pierwsza kopia zapasowa jest zawsze pełna.

Parametr Co tydzień/Co miesiąc powoduje podział całego harmonogramu na harmonogram dzienny, tygodniowy i miesięczny.

Załóżmy, że jako dzień tworzenia tygodniowych/miesięcznych kopii zapasowych wybrano piątek. Poniżej przedstawiono rzeczywisty harmonogram zadań tworzenia kopii zapasowych, które zostaną utworzone.



Zadania tworzenia kopii zapasowych utworzone zgodnie ze schematem GFS przez program Acronis Backup & Recovery 10.
Harmonogram: dni robocze o godz. 20.00
Co tydzień/Co miesiąc: Piątek

Zachowuj kopie zapasowe: Codziennie

Ten krok powoduje zdefiniowanie reguły przechowywania dziennych kopii zapasowych. Po utworzeniu każdej dziennej kopii zapasowej zostanie uruchomione zadanie czyszczenia, które spowoduje usunięcie wszystkich dziennych kopii zapasowych starszych niż określone przez użytkownika.

Zachowuj kopie zapasowe: Co tydzień

Ten krok powoduje zdefiniowanie reguły przechowywania tygodniowych kopii zapasowych. Po utworzeniu każdej tygodniowej kopii zapasowej zostanie uruchomione zadanie czyszczenia, które spowoduje usunięcie wszystkich tygodniowych kopii zapasowych starszych niż określone przez użytkownika. Okres przechowywania tygodniowych kopii zapasowych nie może być krótszy niż okres przechowywania dziennych kopii zapasowych. Zazwyczaj jest on ustawiony jako kilkakrotnie dłuższy.

Zachowuj kopie zapasowe: Co miesiąc

Ten krok powoduje zdefiniowanie reguły przechowywania miesięcznych kopii zapasowych. Po utworzeniu każdej miesięcznej kopii zapasowej zostanie uruchomione zadanie czyszczenia, które spowoduje usunięcie wszystkich miesięcznych kopii zapasowych starszych niż określone przez użytkownika. Okres przechowywania miesięcznych kopii zapasowych nie może być krótszy niż okres przechowywania tygodniowych kopii zapasowych. Zazwyczaj jest on ustawiony jako kilkakrotnie dłuższy. Dostępna jest opcja przechowywania miesięcznych kopii zapasowych w nieskończoność.

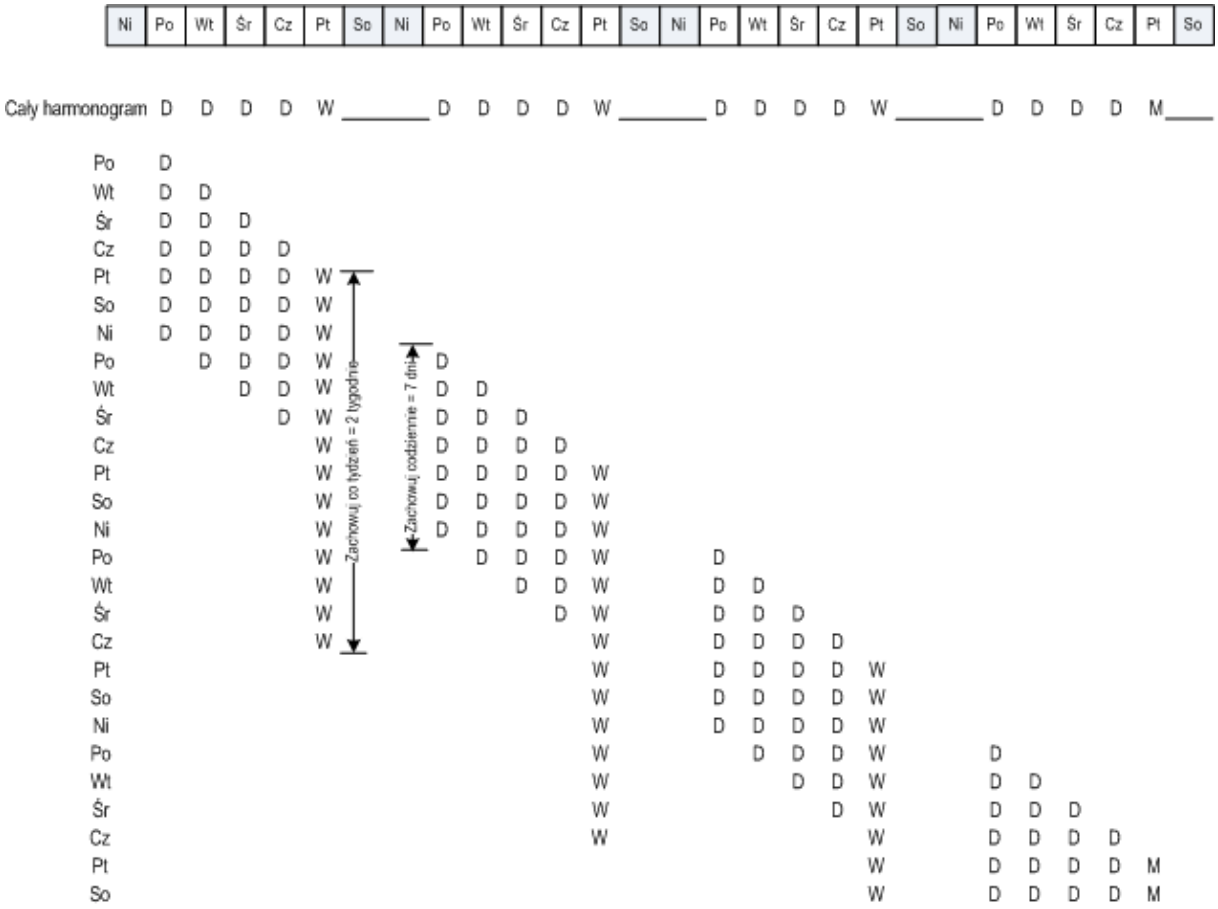
Archiwum wynikowe: idealne

Załóżmy, że wybrano okres przechowywania dziennych kopii zapasowych wynoszący 7 dni, tygodniowych kopii zapasowych — 2 tygodnie, a miesięcznych kopii zapasowych — 6 miesięcy. Poniżej pokazano, jak będzie wyglądało archiwum po uruchomieniu planu tworzenia kopii

zapasowych, jeśli wszystkie kopie zapasowe były pełne i mogły być usuwane, gdy tylko wymagał tego schemat.

W lewej kolumnie znajdują się dni tygodnia. Dla każdego dnia tygodnia pokazano zawartość archiwum po wykonaniu regularnej kopii zapasowej i następującym po nim czyszczeniu.

„D" oznacza kopię zapasową uważaną za dzienną. „W" oznacza kopię zapasową uważaną za tygodniową (ang. „weekly"). „M" oznacza kopię zapasową uważaną za miesięczną.



Idealne archiwum utworzone zgodnie ze schematem GFS.
Harmonogram: dni robocze o godz. 20.00
Co tydzień/Co miesiąc: Piątek
Zachowuj dzienne kopie zapasowe: 7 dni
Zachowuj tygodniowe kopie zapasowe: 2 tygodnie
Zachowuj miesięczne kopie zapasowe: 6 miesięcy

Począwszy od trzeciego tygodnia, tygodniowe kopie zapasowe będą regularnie usuwane. Po upływie 6 miesięcy rozpocznie się usuwanie miesięcznych kopii zapasowych. Diagram dla tygodniowych i miesięcznych kopii zapasowych będzie wyglądał podobnie do schematu dla okresu tygodniowego.

Archiwum wynikowe: rzeczywiste

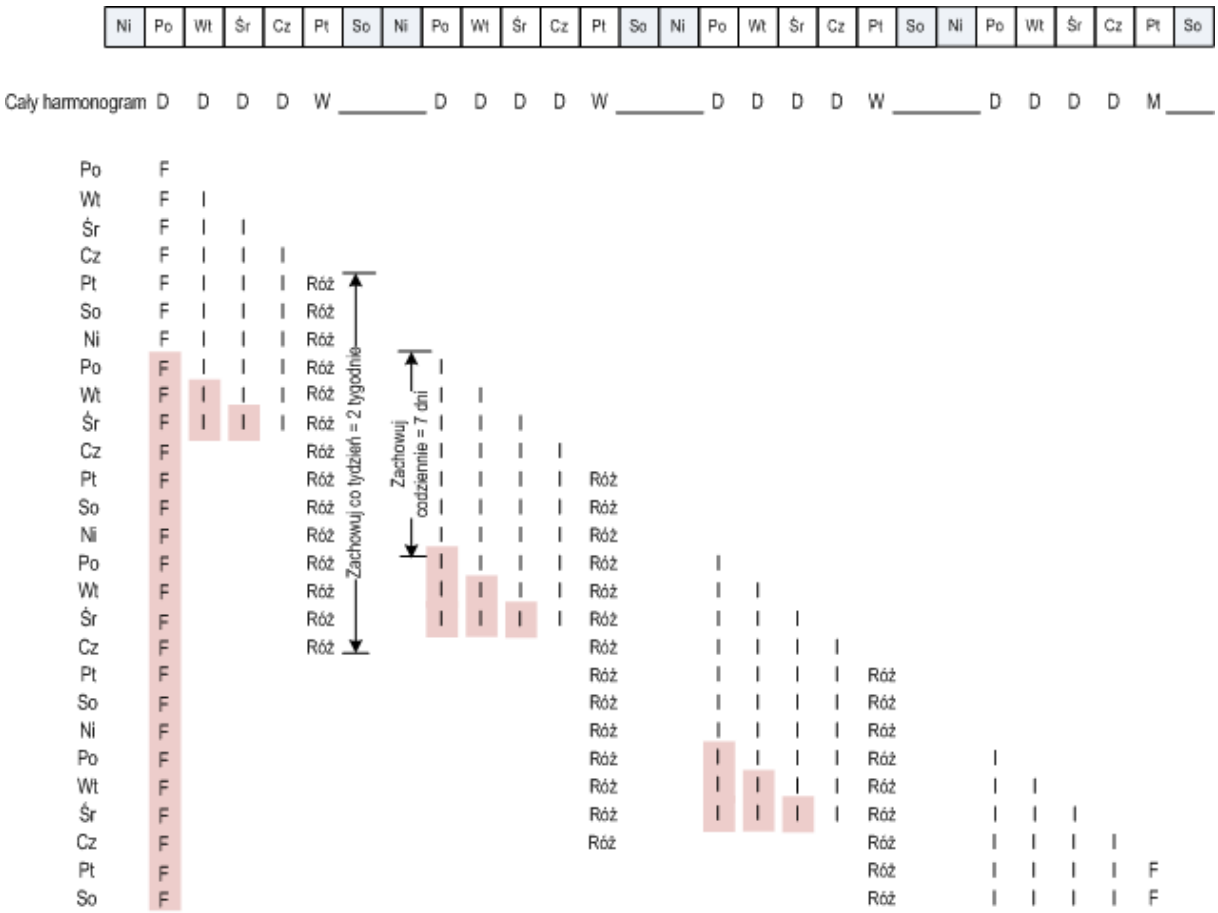
W rzeczywistości zawartość archiwum będzie nieco inna niż w schemacie idealnym.

W przypadku używania przyrostowej i różnicowej metody tworzenia kopii zapasowych nie można usunąć kopii zapasowej, gdy wymaga tego schemat, jeśli na tej kopii zapasowej opierają się kolejne kopie zapasowe. Regularna konsolidacja jest nie do przyjęcia, ponieważ pochłania zbyt dużo zasobów

systemowych. Program musi zaczekać, aż schemat będzie wymagał usunięcia wszystkich zależnych kopii zapasowych. Dopiero wtedy zostanie usunięty cały łańcuch.

Poniżej pokazano, jak będzie wyglądał w rzeczywistości pierwszy miesiąc planu tworzenia kopii zapasowych. „F” oznacza pełną kopię zapasową. „Dif” oznacza różnicową kopię zapasową. „I” oznacza przyrostową kopię zapasową.

Kopie zapasowe, których czas życia przekroczył okres nominalny z powodu zależności, są oznaczone kolorem różowym. Początkowa pełna kopia zapasowa zostanie usunięta natychmiast po usunięciu wszystkich różnicowych i przyrostowych kopii zapasowych opartych na tej kopii zapasowej.



Archiwum utworzone zgodnie ze schematem GFS przez program Acronis Backup & Recovery 10.
Harmonogram: dni robocze o godz. 20.00
Co tydzień/Co miesiąc: Piątek
Zachowuj dzienne kopie zapasowe: 7 dni
Zachowuj tygodniowe kopie zapasowe: 2 tygodnie
Zachowuj miesięczne kopie zapasowe: 6 miesięcy

2.6 Schemat tworzenia kopii zapasowych Wieża Hanoi

Potrzeba częstego tworzenia kopii zapasowych zawsze powoduje konflikty z koniecznością przechowywania takich kopii zapasowych przez długi czas. Rozsądny kompromis zapewnia schemat tworzenia kopii zapasowych Wieża Hanoi.

Przegląd schematu Wieża Hanoi

Schemat Wieża Hanoi jest oparty na matematycznej układance o tej samej nazwie. Kilka pierścieni jest ułożonych kolejno według wielkości na jednym z trzech kołków. Największy pierścień znajduje się na dole. Celem układanki jest przeniesienie wszystkich pierścieni na trzeci kołek. Jednocześnie można przenieść tylko jeden pierścień, ale nie można umieścić większego pierścienia nad mniejszym. Rozwiązanie polega na przenoszeniu pierwszego pierścienia co drugi ruch (ruchy 1, 3, 5, 7, 9, 11...), drugiego pierścienia co cztery ruchy (ruchy 2, 6, 10...), trzeciego pierścienia co osiem ruchów (ruchy 4, 12...) itd.

Jeśli na przykład w układance istnieje pięć pierścieni oznaczonych A, B, C, D i E, rozwiązanie wymaga następującej kolejności ruchów:

Przenieś / Zadzwoń	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
1	A		A		A		A		A		A		A		A		A		A		A		A		A		A		A		A
2		B				B				B				B				B				B				B				B	
3				C								C								C								C			
4								D																D							
5																E															

Schemat tworzenia kopii zapasowych Wieża Hanoi opiera się na tym sam wzorcu. Zamiast **ruchów** stosowane są **sesje**, a zamiast **pierścieni** — **poziomy tworzenia kopii zapasowych**. Typowy wzorzec schematu z N poziomami składa się z (2 do potęgi N) sesji.

Oznacza to, że schemat tworzenia kopii zapasowych Wieża Hanoi z pięcioma poziomami ma cykliczny wzorzec składający się z 16 sesji (ruchy od 1 do 16 na powyższym rysunku).

Tabela przedstawia wzorzec dla schematu tworzenia kopii zapasowych z pięcioma poziomami. Wzorzec składa się z 16 sesji.

Poziom tworzenia kopii zapasowej / Sesja	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	A		A		A		A		A		A		A		A	
2		B				B				B				B		
3				C								C				
4								D								
5																E

Schemat tworzenia kopii zapasowych Wieża Hanoi nakazuje istnienie tylko jednej kopii zapasowej na każdym poziomie. Wszystkie przestarzałe kopie zapasowe muszą być usunięte. Oznacza to, że ten schemat zapewnia wydajne składowanie danych, ponieważ przechowywana jest większa liczba kopii zapasowych aktualnych danych. W przypadku czterech kopii zapasowych można odzyskać dane z bieżącego dnia, z poprzedniego dnia, sprzed połowy tygodnia i sprzed tygodnia. Schemat z pięcioma poziomami umożliwia także odzyskanie danych sprzed dwóch tygodni. Każdy dodatkowy poziom kopii zapasowej podwaja maksymalny okres przywracania danych.

Schemat Wieża Hanoi w programach Acronis

Schemat tworzenia kopii zapasowych Wieża Hanoi jest zbyt skomplikowany, aby samodzielnie obliczać, który nośnik powinien zostać użyty jako następny. Program Acronis Backup & Recovery 10

zapewnia automatyzację sposobu użycia schematu. Schemat tworzenia kopii zapasowych można skonfigurować podczas przygotowywania planu tworzenia kopii zapasowych.

W programach Acronis schemat ma następujące funkcje:

- do 16 poziomów tworzenia kopii zapasowych;
- tworzenie przyrostowych kopii zapasowych na pierwszym poziomie (A), aby oszczędzić czas i miejsce podczas najczęściej wykonywanych operacji tworzenia kopii zapasowych; jednak odzyskanie danych z takich kopii zapasowych zajmuje więcej czasu, ponieważ zwykle wymaga dostępu do trzech kopii zapasowych;
- tworzenie pełnych kopii zapasowych na ostatnim poziomie (E w przypadku wzorca z pięcioma poziomami) — są to najrzadziej wykonywane kopie zapasowe w tym schemacie, które wymagają najwięcej czasu i miejsca na pamięci masowej;
- tworzenie różnicowych kopii zapasowych na wszystkich poziomach pośrednich (B, C i D w przypadku wzorca z pięcioma poziomami);
- wzorzec zaczyna się od pełnej kopii zapasowej, ponieważ pierwsza kopia zapasowa nie może być przyrostowa;
- schemat wymusza, aby na każdym poziomie zachować tylko najbardziej aktualną kopię zapasową; inne kopie zapasowe na danym poziomie muszą zostać usunięcie, ale usuwanie kopii zapasowych zostaje opóźnione w przypadku, gdy dana kopia zapasowa stanowi podstawę dla innej przyrostowej lub różnicowej kopii zapasowej;
- stara kopia zapasowa na danym poziomie zostaje zachowana do momentu pomyślnego utworzenia nowej kopii zapasowej na tym poziomie.

Tabela przedstawia wzorzec dla schematu tworzenia kopii zapasowych z pięcioma poziomami. Wzorzec składa się z 16 sesji.

Poziom tworzenia kopii zapasowej \ Sesja	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1 (Przyrostowa)		A		A		A		A		A		A		A		A
2 (Różnicowa)			B				B				B				B	
3 (Różnicowa)					C								C			
4 (Różnicowa)									D							
5 (Pełna)	E															

W wyniku użycia przyrostowych i różnicowych kopii zapasowych może wystąpić sytuacja, w której konieczne będzie opóźnienie usunięcia starej kopii zapasowej, jeśli stanowi ona podstawę dla innych kopii zapasowych. Poniższa tabela przedstawia przypadek, w którym usunięcie pełnej kopii zapasowej (E) utworzonej w czasie sesji 1 zostanie opóźnione w sesji 17 aż do sesji 25, ponieważ różnicowa kopia zapasowa (D) utworzona w czasie sesji 9 ciągle będzie aktualna. Wszystkie komórki tabeli z usuniętymi kopiami zapasowymi są wyszarzone:

Poziom tworzenia kopii zapasowej \ Sesja	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
1 (Przyrostowa)		A		A		A		A		A		A		A		A		A		A		A		A	
2 (Różnicowa)			B				B				B				B				B				B		
3 (Różnicowa)					C								C								C				
4 (Różnicowa)									D																D
5 (Pełna)	E																E								

Różnicowa kopia zapasowa (D) utworzona w czasie sesji 9 zostanie usunięta podczas sesji 25 po zakończeniu tworzenia nowej różnicowej kopii zapasowej. Oznacza to, że archiwum kopii zapasowej utworzone z użyciem schematu Wieża Hanoi w programie Acronis niekiedy zawiera do dwóch dodatkowych kopii zapasowych w stosunku do klasycznej implementacji schematu.

Więcej informacji na temat użycia schematu Wieża Hanoi dla bibliotek taśm zawiera sekcja Użycie schematu rotacji taśm Wieża Hanoi (s. 170).

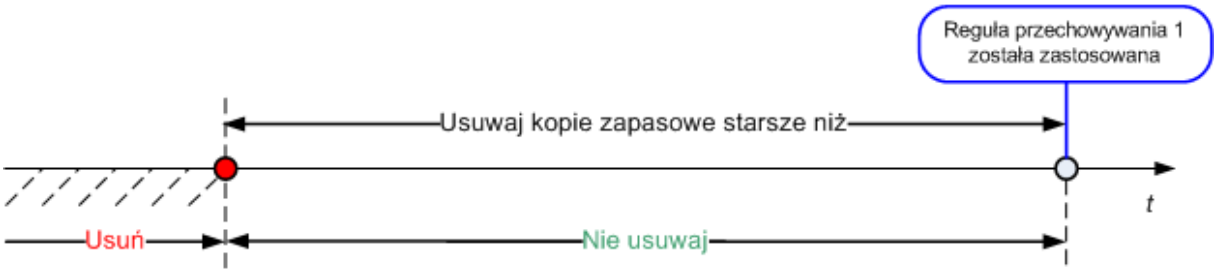
2.7 Reguły przechowywania

Kopie zapasowe utworzone na podstawie planu tworzenia kopii zapasowych składają się na archiwum. Dwie reguły przechowywania opisane w tej sekcji umożliwiają ograniczenie rozmiaru archiwum i ustawienie czasu istnienia (okresu przechowywania) kopii zapasowych.

Reguły przechowywania są stosowane, jeśli archiwum zawiera więcej niż jedną kopię zapasową. Oznacza to, że ostatnia kopia zapasowa w archiwum zostanie zachowana nawet wtedy, gdy naruszy to regułę przechowywania. Nie próbuj usuwać jedynej posiadanej kopii zapasowej przez zastosowanie reguł przechowywania *przed* tworzeniem kopii. Taka próba się nie powiedzie. Jeśli akceptujesz ryzyko utraty ostatniej kopii zapasowej, użyj ustawienia alternatywnego **Wyczyść archiwum** > **Kiedy jest za mało miejsca podczas tworzenia kopii zapasowej** (s. 243).

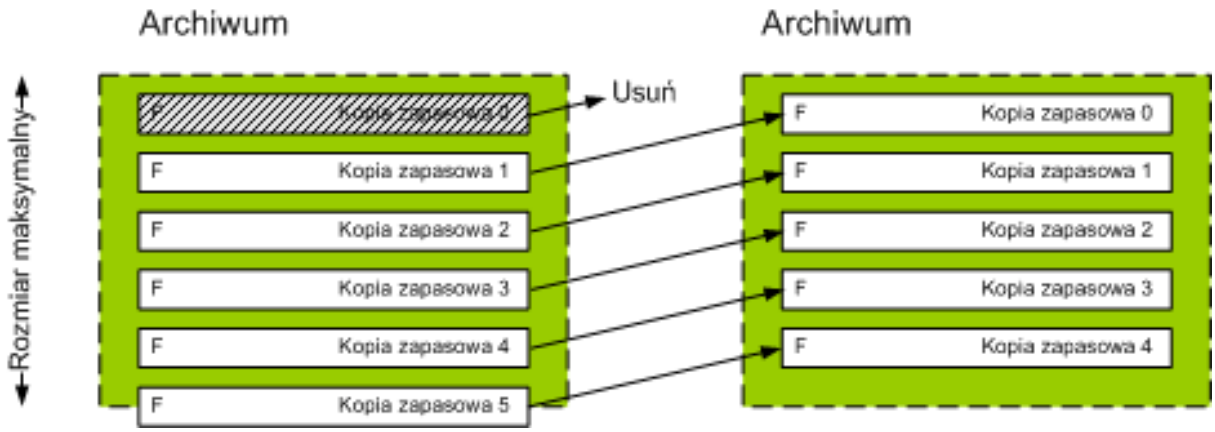
1. Usuwaj kopie zapasowe starsze niż

Jest to przedział czasu odliczany od momentu zastosowania reguł przechowywania. Każde zastosowanie reguły przechowywania powoduje, że program oblicza datę i godzinę w przeszłości odpowiadającą temu przedziałowi oraz usuwa wszystkie kopie zapasowe utworzone przed tym czasem. Żadna kopia zapasowa utworzona po tym czasie nie zostanie usunięta.

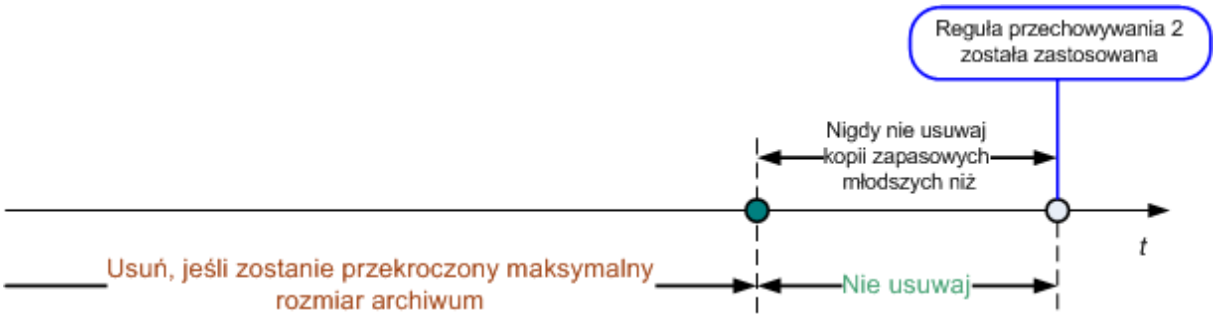


2. Utrzymuj rozmiar archiwum w granicach

Jest to maksymalny rozmiar archiwum. Każde zastosowanie reguły przechowywania powoduje, że program porównuje rzeczywisty rozmiar archiwum z ustawioną wartością i usuwa najstarsze kopie zapasowe, aby rozmiar archiwum nie przekraczał tej wartości. Na poniższym diagramie pokazano zawartość archiwum przed usunięciem i po nim.

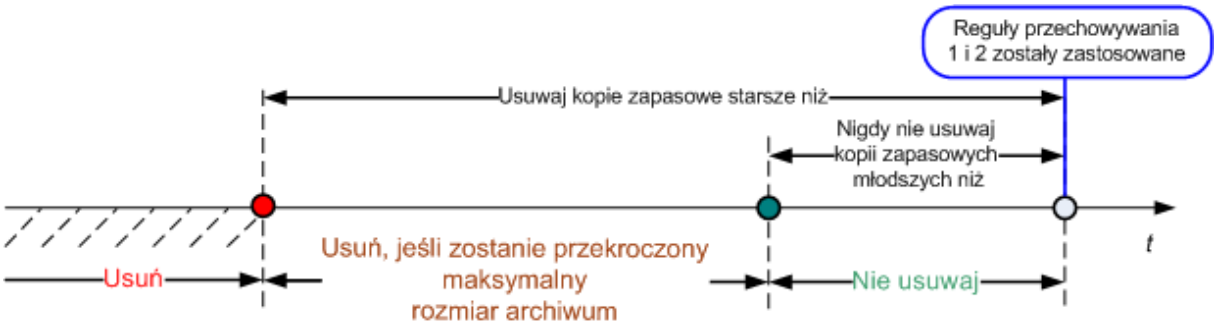


Istnieje pewne ryzyko, że w przypadku niewłaściwego (zbyt małego) ustawienia maksymalnego rozmiaru archiwum zostaną usunięte wszystkie kopie zapasowe oprócz jednej lub regularna kopia zapasowa okaże się zbyt duża. Aby zabezpieczyć najnowsze kopie zapasowe przed usunięciem, należy zaznaczyć pole wyboru **Nigdy nie usuwaj kopii zapasowych młodszych niż** i określić maksymalny wiek kopii zapasowych, które muszą być przechowywane. Poniższy diagram ilustruje regułę wynikową.



Połączenie reguł 1 i 2

Ograniczyć można zarówno czas istnienia kopii zapasowych, jak i rozmiar archiwum. Poniższy diagram ilustruje regułę wynikową.



Przykład

Usuwaj kopie zapasowe starsze niż = 3 miesiące

Utrzymuj rozmiar archiwum w granicach = 200 GB

Nigdy nie usuwaj kopii zapasowych młodszych niż = 10 dni

- Każde zastosowanie reguł przechowywania powoduje, że program usuwa wszystkie kopie zapasowe utworzone wcześniej niż przed 3 miesiącami (a dokładniej — 90 dniami).
- Jeśli po usunięciu rozmiar archiwum jest większy niż 200 GB, a najstarsza kopia zapasowa jest starsza niż 10 dni, program usuwa tę kopię.
- Następnie w razie potrzeby usuwana jest kolejna stara kopia zapasowa. Dzieje się tak, dopóki rozmiar archiwum nie zmniejszy się do ustawionego limitu lub dopóki wiek najstarszej kopii zapasowej nie osiągnie 10 dni.

Usuwanie kopii zapasowych z zależnościami

Obie reguły przechowywania zakładają usuwanie niektórych kopii zapasowych i zachowywanie innych. Co jednak dzieje się w przypadku, gdy archiwum zawiera przyrostowe i różnicowe kopie zapasowe zależne od siebie nawzajem oraz od pełnych kopii zapasowych, na podstawie których zostały utworzone? Nie można na przykład usunąć przestarzałej pełnej kopii zapasowej i zachować jej przyrostowych kopii podrzędnych.

Gdy usunięcie jednej kopii zapasowej wpływa na inne kopie zapasowe, stosowana jest jedna z następujących reguł:

- **Przechowuj kopię zapasową, dopóki nie zostaną usunięte wszystkie zależne kopie zapasowe**

  Przestarzała kopia zapasowa będzie przechowywana do momentu, gdy wszystkie zależne od niej kopie zapasowe także staną się przestarzałe. Następnie podczas regularnego czyszczenia cały łańcuch zostanie usunięty jednocześnie. Ten tryb pomaga uniknąć ewentualnej czasochłonnej konsolidacji, ale wymaga dodatkowego miejsca na przechowywanie kopii zapasowych, których usunięcie zostało opóźnione. Rozmiar archiwum lub wiek kopii zapasowych może przekroczyć wartości określone przez użytkownika.
- **Konsoliduj kopie zapasowe**

  Program skonsoliduje kopię zapasową przeznaczoną do usunięcia z następną zależną od niej kopią zapasową. Załóżmy na przykład, że reguły przechowywania wymagają usunięcia pełnej kopii zapasowej i zachowania następnej kopii przyrostowej. Kopie zapasowe zostaną scalone w jedną pełną kopię zapasową, która jako datę utworzenia otrzyma datę utworzenia

przyrostowej kopii zapasowej. Po usunięciu przyrostowej lub różnicowej kopii zapasowej ze środka łańcucha wynikowa kopia zapasowa będzie kopią przyrostową.

Ten tryb gwarantuje, że po każdym czyszczeniu rozmiar archiwum i wiek kopii zapasowych będą się mieściły w granicach określonych przez użytkownika. Jednak konsolidacja może pochłonąć mnóstwo czasu i zasobów systemowych. Poza tym w skarbcu będzie potrzebne dodatkowe miejsce na pliki tymczasowe tworzone podczas konsolidacji.

Co trzeba wiedzieć o konsolidacji

Należy pamiętać, że konsolidacja to jedynie metoda usuwania, a nie alternatywa dla usuwania. Wynikowa kopia zapasowa nie będzie zawierać danych, które były obecne w usuniętej kopii zapasowej, a których nie było w zachowanej przyrostowej lub różnicowej kopii zapasowej.

Kopie zapasowe otrzymane w wyniku konsolidacji zawsze mają maksymalną kompresję. Oznacza to, że w rezultacie wielokrotnego czyszczenia z zastosowaniem konsolidacji wszystkie kopie zapasowe w archiwum mogą osiągnąć maksymalną kompresję.

Sprawdzone praktyki

Należy zachować równowagę między pojemnością urządzenia pamięci, ustawionymi parametrami ograniczającymi oraz częstotliwością czyszczenia. Logika reguł przechowywania zakłada, że pojemność urządzenia pamięci jest dużo większa niż średni rozmiar kopii zapasowej, a maksymalny rozmiar archiwum jest na tyle odległy od fizycznej pojemności urządzenia pamięci, że zapewnia odpowiedni zapas. Dzięki temu przekroczenie rozmiaru archiwum, które może się zdarzyć między uruchomieniami zadania czyszczenia, nie będzie miało krytycznego znaczenia dla całego procesu. Im rzadziej uruchamiane jest zadanie czyszczenia, tym więcej miejsca potrzeba na przechowywanie kopii zapasowych, które przekroczyły swój nominalny czas istnienia.

Na stronie Skarbce (s. 144) znajdują się informacje o wolnym miejscu dostępnym w poszczególnych skarbcach. Od czasu do czasu warto zaglądać na tę stronę. Jeśli wolne miejsce (które tak naprawdę oznacza wolne miejsce w urządzeniu pamięci) zbliża się do zera, być może trzeba zaostrzyć ograniczenia dotyczące niektórych lub wszystkich archiwów znajdujących się w danym skarbcu.

2.8 Tworzenie kopii zapasowych woluminów dynamicznych (Windows)

W tej sekcji omówiono w zarysie, jak tworzyć kopie zapasowe i odzyskiwać woluminy dynamiczne (s. 431) przy użyciu programu Acronis Backup & Recovery 10. Omówiono także podstawowe dyski korzystające z tabeli partycji GUID (GUID Partition Table — GPT).

Wolumin dynamiczny to wolumin znajdujący się na dyskach dynamicznych (s. 420), a dokładniej w grupie dysków (s. 422). Program Acronis Backup & Recovery 10 obsługuje następujące typy woluminów dynamicznych/poziomy macierzy RAID:

- prosty/łączony,
- rozłożony (RAID 0),
- lustrzany (RAID 1),
- lustrzany-rozłożony (RAID 0+1),
- RAID 5.

Program Acronis Backup & Recovery 10 umożliwia tworzenie kopii zapasowych i odzyskiwanie woluminów dynamicznych oraz (z niewielkimi ograniczeniami) podstawowych woluminów GPT.

Tworzenie kopii zapasowych woluminów dynamicznych

Kopie zapasowe woluminów dynamicznych i podstawowych woluminów GPT są tworzone tak samo jak kopie podstawowych woluminów MBR. Podczas definiowania planu tworzenia kopii zapasowych za pośrednictwem graficznego interfejsu użytkownika wszystkie typy woluminów są dostępne do wyboru jako **Elementy uwzględniane w kopii zapasowej**. W przypadku korzystania z wiersza polecenia woluminy dynamiczne i woluminy GPT należy określić za pomocą prefiksu DYN.

Przykłady wiersza polecenia

```
trueimagecmd /create /partition:DYN1,DYN2 /asz
```

Spowoduje to utworzenie kopii zapasowej woluminów DYN1 i DYN2 w strefie Acronis Secure Zone.

```
trueimagecmd /create /harddisk:DYN /asz
```

Spowoduje to utworzenie kopii zapasowej wszystkich woluminów dynamicznych systemu w strefie Acronis Secure Zone.

Nie można utworzyć kopii zapasowej kodu startowego podstawowych woluminów GPT ani go odzyskać.

Odzyskiwanie woluminów dynamicznych

Wolumin dynamiczny można odzyskać:

- na istniejącym woluminie dowolnego typu,
- do nieprzydzielonego miejsca w grupie dysków,
- do nieprzydzielonego miejsca na dysku podstawowym.

Odzyskiwanie na istniejącym woluminie

Gdy wolumin dynamiczny jest odzyskiwany na istniejącym woluminie (podstawowym lub dynamicznym), dane na woluminie docelowym są zastępowane zawartością kopii zapasowej. Typ woluminu docelowego (podstawowy, prosty/łączony, rozłożony, lustrzany, RAID 0+1, RAID 5) nie ulega zmianie. Rozmiar woluminu docelowego musi być wystarczający, aby pomieścić zawartość kopii zapasowej.

Odzyskiwanie do nieprzydzielonego miejsca w grupie dysków

Gdy wolumin dynamiczny jest odzyskiwany do nieprzydzielonego miejsca w grupie dysków, odzyskiwany jest zarówno typ, jak i zawartość woluminu wynikowego. Rozmiar nieprzydzielonego miejsca musi być wystarczający, aby pomieścić zawartość kopii zapasowej. Ważny jest także rozkład nieprzydzielonego miejsca między dyskami.

Przykład

Woluminy rozłożone zużywają równą ilość miejsca na każdym dysku.

Załóżmy, że wolumin rozłożony o rozmiarze 30 GB ma zostać odzyskany do grupy dysków obejmującej dwa dyski. Każdy dysk zawiera woluminy i pewną ilość nieprzydzielonego miejsca. Całkowity rozmiar nieprzydzielonego miejsca wynosi 40 GB. Jeśli nieprzydzielone miejsce jest rozłożone między dyskami równomiernie (20 GB i 20 GB), w wyniku odzyskiwania zawsze powstanie wolumin rozłożony.

Jeśli na jednym dysku znajduje się 10 GB, a na drugim 30 GB nieprzydzielonego miejsca, wynik odzyskiwania zależy od rozmiaru odzyskiwanych danych.

- Jeśli rozmiar danych jest mniejszy niż 20 GB, na jednym dysku może znaleźć się na przykład 10 GB, a na drugim pozostałe 10 GB. W ten sposób na obu dyskach zostanie utworzony wolumin rozłożony, a 20 GB na drugim dysku pozostanie nieprzydzielone.

- Jeśli rozmiar danych jest większy niż 20 GB, nie można ich rozłożyć równomiernie między dwoma dyskami, ale zmieszczą się one na pojedynczym woluminie prostym. Wolumin prosty zawierający wszystkie dane zostanie utworzony na drugim dysku. Pierwszy dysk pozostanie bez zmian.

	Przedmiot (źródło) kopii zapasowej:		
Miejsce odzyskiwania:	**Wolumin dynamiczny**	**Podstawowy wolumin MBR**	**Podstawowy wolumin GPT**
Wolumin dynamiczny	Wolumin dynamiczny Takiego samego typu jak miejsce docelowe	Wolumin dynamiczny Takiego samego typu jak miejsce docelowe	Wolumin dynamiczny Takiego samego typu jak miejsce docelowe
Nieprzydzielone miejsce (grupa dysków)	Wolumin dynamiczny Takiego samego typu jak źródło	Wolumin dynamiczny Prosty	N/D
Podstawowy wolumin MBR	Podstawowy wolumin MBR	Podstawowy wolumin MBR	Podstawowy wolumin MBR
Podstawowy wolumin GPT	Podstawowy wolumin GPT	Podstawowy wolumin GPT	Podstawowy wolumin GPT
Nieprzydzielone miejsce (podstawowy dysk MBR)	Podstawowy wolumin MBR	Podstawowy wolumin MBR	Podstawowy wolumin MBR
Nieprzydzielone miejsce (podstawowy dysk GPT)	Podstawowy wolumin GPT	Podstawowy wolumin GPT	Podstawowy wolumin GPT

Przenoszenie i zmiana rozmiaru woluminów podczas odzyskiwania

Podczas odzyskiwania można zmienić rozmiar wynikowego woluminu podstawowego (zarówno MBR, jak i GPT) lub zmienić jego lokalizację na dysku. Nie można zmienić lokalizacji ani rozmiaru wynikowego woluminu dynamicznego.

Przygotowywanie grup dysków i woluminów

Przed odzyskiwaniem woluminów dynamicznych od podstaw należy na sprzęcie docelowym utworzyć grupę dysków.

Może być także konieczne utworzenie lub zwiększenie nieprzydzielonego miejsca w istniejącej grupie dysków. W tym celu można usunąć woluminy lub przekonwertować dyski podstawowe na dynamiczne.

Można zmienić typ woluminu docelowego (podstawowy, prosty/łączony, rozłożony, lustrzany, RAID 0+1, RAID 5). W tym celu należy usunąć wolumin docelowy i w uzyskanym nieprzydzielonym miejscu utworzyć nowy wolumin.

Program Acronis Backup & Recovery 10 zawiera wygodne narzędzie do zarządzania dyskami, które umożliwia wykonanie powyższych operacji zarówno w systemie operacyjnym, jak i na nowym sprzęcie bez systemu operacyjnego. Więcej informacji na temat narzędzia Acronis Disk Director Lite można znaleźć w sekcji Zarządzanie dyskami (s. 309)

2.9 Tworzenie kopii zapasowych woluminów LVM i urządzeń MD (Linux)

W tej sekcji został przedstawiony sposób tworzenia kopii zapasowych oraz odzyskiwania woluminów zarządzanych przez menedżer dysków logicznych systemu Linux (ang. Logical Volume Manager, LVM)

nazywanych woluminami logicznymi, oraz urządzeń z wieloma dyskami (ang. multiple-disk, MD) nazywanych programowymi urządzeniami RAID systemu Linux.

2.9.1 Tworzenie kopii zapasowych woluminów logicznych

Komponent Acronis Backup & Recovery 10 Agent dla systemu Linux umożliwia dostęp do takich woluminów, tworzenie ich kopii zapasowych oraz ich odzyskiwanie w systemie Linux z jądrem 2.6.x lub przy użyciu nośnika startowego opartego na systemie Linux.

Kopia zapasowa (graficzny interfejs użytkownika)

W graficznym interfejsie użytkownika programu Acronis Backup & Recovery 10 woluminy logiczne są wyświetlane w sekcji **Woluminy dynamiczne i GPT** na końcu listy woluminów dostępnych do tworzenia kopii zapasowych.

Aby utworzyć kopię zapasową wszystkich dostępnych dysków, należy określić wszystkie woluminy logiczne oraz nienależące do nich woluminy podstawowe. Jest to opcja domyślna po otwarciu strony **Utwórz plan tworzenia kopii zapasowych**.

Na liście wyświetlane są woluminy podstawowe zawarte w woluminach logicznych, oznaczone jako **Brak** w kolumnie **System plików**. Jeśli wybierzesz takie woluminy, program będzie tworzył ich kopie zapasowe metodą „sektor po sektorze”. Zwykle nie jest to wymagane.

Odzyskiwanie

W przypadku odzyskiwania woluminów logicznych dostępne są dwie opcje:

- **Odzyskiwanie tylko zawartości woluminów**. Typ i inne właściwości woluminu docelowego nie ulegają zmianie.

  Ta opcja jest dostępna zarówno po uruchomieniu programu w systemie operacyjnym, jak i przy użyciu nośnika startowego.

  Ta opcja jest przydatna w następujących przypadkach:

  - Gdy nastąpiła utrata części danych z woluminu, ale nie wymieniono dysków twardych.
  - Podczas odzyskiwania woluminu logicznego na podstawowy dysk lub wolumin (MBR). W takim przypadku możesz zmienić rozmiar woluminu wynikowego.

    Nie jest możliwe uruchomienie systemu odzyskanego z woluminu logicznego na podstawowy dysk MBR, ponieważ jądro systemu próbuje zamontować główny system plików na woluminie logicznym. Aby uruchomić system, należy zmienić konfigurację programu ładującego i plik /etc/fstab, tak aby nie było używane narzędzie LVM, a następnie aktywować ponownie program ładujący (s. 267).

  - Podczas odzyskiwania woluminu podstawowego lub logicznego na utworzony wcześniej wolumin logiczny. Taka sytuacja może wystąpić, gdy utworzysz strukturę woluminów logicznych ręcznie przy użyciu narzędzia **lvm**.
- **Odzyskiwanie struktury oraz zawartości woluminów logicznych**.

  Taka sytuacja może wystąpić podczas odzyskiwania na komputerze bez zainstalowanego systemu operacyjnego, lub na komputerze o innej strukturze woluminów. Strukturę woluminów logicznych można automatycznie utworzyć podczas odzyskiwania, jeśli została zapisana w kopii zapasowej (s. 52).

  Ta opcja jest dostępna tylko podczas pracy z nośnikiem startowym.

Szczegółowe instrukcje dotyczące odzyskiwania woluminów logicznych zawiera sekcja Odzyskiwanie urządzeń MD i woluminów logicznych (s. 304).

Przydatne łącze:

- http://tldp.org/HOWTO/LVM-HOWTO/.

2.9.2 Tworzenie kopii zapasowych urządzeń MD

Urządzenia MD łączą kilka woluminów i stanowią urządzenia blokowe (/dev/md0, /dev/md1, ..., /dev/md31). Informacje na temat urządzeń MD są przechowywane w katalogu /etc/raidtab lub w wydzielonych obszarach tych woluminów.

Kopie zapasowe aktywnych (zamontowanych) urządzeń MD można tworzyć w taki sam sposób jak kopie woluminów logicznych. Urządzenia MD znajdują się na końcu listy woluminów dostępnych do utworzenia kopii zapasowej.

Tworzenie kopii zapasowych woluminów znajdujących się na zamontowanych urządzeniach MD nie ma sensu, ponieważ ich odzyskanie będzie niemożliwe.

Podczas odzyskiwania urządzeń MD przy użyciu nośnika startowego możesz automatycznie odtworzyć ich strukturę, jeśli została ona zapisana w kopii zapasowej (s. 52). Aby uzyskać szczegółowe informacje na temat odzyskiwania urządzeń MD przy użyciu nośnika startowego, zobacz Odzyskiwanie urządzeń MD i woluminów logicznych (s. 304).

Aby uzyskać informacje na temat składania urządzeń MD podczas odzyskiwania w systemie Linux, zobacz Składanie urządzeń MD do odzyskiwania (Linux) (s. 269).

2.9.3 Zapisywanie informacji o strukturze woluminu

Aby po odzyskaniu automatycznie odtworzyć strukturę urządzeń MD i woluminów logicznych, należy zapisać informacje o strukturze woluminów w jeden z następujących sposobów:

- Podczas tworzenia planu tworzenia kopii zapasowych na poziomie dysków przejdź do opcji **Opcje tworzenia kopii zapasowych > Ustawienia zaawansowane** i zaznacz pole wyboru **Razem z kopiami zapasowymi zapisz metadane programowej macierzy RAID i woluminu LVM**. (To pole jest domyślnie zaznaczone).
- Przed wykonaniem pierwszej kopii zapasowej dysku na komputerze źródłowym uruchom następujące polecenie:

```
trueimagecmd --dumpraidinfo
```

Obie te operacje powodują zapisanie struktury logicznej woluminów w komputerze w katalogu /etc/Acronis. Upewnij się, że wolumin, na którym znajduje się ten katalog, został wybrany do utworzenia kopii zapasowej.

2.9.4 Wybieranie woluminów logicznych i urządzeń MD w wierszu polecenia

Przyjmijmy, że w komputerze znajdują się cztery dyski fizyczne: Dysk 1, Dysk 2, Dysk 3 i Dysk 4.

- Wolumin RAID-1 jest skonfigurowany na dwóch woluminach podstawowych: sdb1, sdd1
- Wolumin logiczny jest skonfigurowany na dwóch woluminach podstawowych: sdb2, sdd2
- Dysk 1 zawiera strefę Acronis Secure Zone, która zwykle nie jest uwzględniana w kopii zapasowej.

Listę woluminów można wyświetlić, używając następującego polecenia:

```
trueimagecmd --list
```



```
Num  Partition             Flags       Start      Size       Type
---- -------------------- ----------- ---------- ---------- -----------
Disk 1 (sda):
1-1  sda1                 Pri,Act     63         208813     Ext2
1-2  sda2                 Pri         417690     12289725   ReiserFS
1-3  sda3                 Pri         24997140   1052257    Linux Swap
     Unallocated                      27101655   2698920    Unallocated
1-4  Acronis Secure Zone  Pri         32499495   522112     FAT32
     Unallocated                      33543720   5356       Unallocated
Disk 2 (sdb):
2-1  sdb1                 Pri         62         124969     Ext2
2-2  sdb2                 Pri         250001     125000     None
     Unallocated                      500001     8138607    Unallocated
Disk 3 (sdc):
     Table                            0                     Table
     Unallocated                      1          1048575    Unallocated
Disk 4 (sdd):
4-1  sdd1                 Pri         62         124969     Ext2
4-2  sdd2                 Pri         250001     125000     None
     Unallocated                      500001     798575     Unallocated
Woluminy dynamiczne i GPT:
DYN1  VolGroup00-LogVol00                        245760     Ext3
                          Disk: 3     250385     245760
                          Disk: 5     250385     245760
DYN2  md0                                        124864     Ext2
                          Disk: 5     62         249728
                          Disk: 3     62         249728
```

Wolumin logiczny DYN1 znajduje się na woluminach podstawowych 2-2 i 4-2. Wolumin RAID-1 DYN2 znajduje się na woluminach podstawowych 2-1 i 4-1.

Aby utworzyć kopię zapasową woluminu logicznego DYN1, uruchom następujące polecenie (przyjęto nazwę kopii zapasowej: /home/backup.tib):

```
trueimagecmd --partition:dyn1 --filename:/home/backup.tib --create
```

Aby utworzyć kopię zapasową woluminu RAID-1 DYN2, uruchom następujące polecenie:

```
trueimagecmd --partition:dyn2 --filename:/home/backup.tib --create
```

Aby utworzyć kopię zapasową wszystkich trzech dysków twardych z woluminami, wybierz woluminy 1-1, 1-2, 1-3, DYN1 i DYN2:

```
trueimagecmd --partition:1-1,1-2,1-3,dyn1,dyn2 --filename:/home/backup.tib --
create
```

Jeśli zostanie wybrany Dysk 3, wolumin 2-1 lub wolumin 2-2, program utworzy kopię zapasową surowych danych (sektor po sektorze).

2.10 Tworzenie kopii zapasowych sprzętowych macierzy RAID (Linux)

Sprzętowe macierze RAID w systemie Linux łączą kilka dysków fizycznych, tworząc pojedynczy dysk, który można podzielić na partycje. Specjalny plik związany ze sprzętową macierzą RAID zazwyczaj znajduje się w katalogu /dev/ataraid. Kopie zapasowe sprzętowych macierzy RAID można tworzyć w taki sam sposób jak kopie zapasowe zwykłych dysków twardych.

Dyski fizyczne wchodzące w skład sprzętowych macierzy RAID mogą być wyświetlane obok innych dysków tak, jakby miały nieprawidłową tabelę partycji lub w ogóle nie miały tabeli partycji. Tworzenie kopii zapasowych takich dysków nie ma sensu, ponieważ ich odzyskanie będzie niemożliwe.

2.11 Tworzenie kopii zapasowych maszyn wirtualnych

Program Acronis Backup & Recovery 10 Advanced Server Virtual Edition umożliwia tworzenie kopii zapasowych maszyn wirtualnych z poziomu hosta.

Przygotowanie

W systemie Windows 2008 Server x64 (dowolnej wersji) lub Microsoft Hyper-V Server 2008:

- Zainstaluj na hoście Hyper-V agenta dla systemu Hyper-V.
- W systemach-gościach muszą być zainstalowane usługi integracji (s. 56).

W systemie VMware ESX/ESXi:

- Zainstaluj Agenta dla ESX/ESXi na hoście ESX lub ESXi. Agent jest dostarczany jako urządzenie wirtualne.
- W systemach-gościach muszą być zainstalowane narzędzia VMware (s. 56).

Tworzenie kopii zapasowych maszyn wirtualnych

Po zainstalowaniu agenta na hoście oraz wymaganych usług w systemach-gościach można:

- Tworzyć kopie zapasowe maszyn wirtualnych znajdujących się na serwerze bez konieczności instalowania agenta na każdej maszynie.
- Odzyskiwać maszyny wirtualne na tej samej, innej lub nowej maszynie wirtualnej, znajdującej się na tym samym serwerze lub na innym serwerze wirtualizacji, na którym zainstalowany jest agent dla maszyn wirtualnych. Konfiguracja maszyny wirtualnej zapisana w kopii zapasowej jest proponowana jako domyślna podczas odzyskiwania zawartości kopii na nowej maszynie wirtualnej.
- Tworzyć i odzyskiwać kopie zapasowe poszczególnych dysków i woluminów maszyny wirtualnej.

Podczas tworzenia kopii zapasowej maszyna wirtualna może być w trybie online (działać), offline (nie działać), być wstrzymana albo zmieniać swój tryb.

Podczas odzyskiwania maszyna wirtualna musi być w trybie offline (nie może działać). Przed odzyskaniem maszyna jest automatycznie zatrzymywana. Można wybrać opcję ręcznego zatrzymywania maszyn (s. 142).

Kopia zapasowa maszyny wirtualnej a kopia zapasowa woluminów maszyny

Tworzenie kopii zapasowej maszyny wirtualnej oznacza tworzenie kopii zapasowej wszystkich dysków tej maszyny oraz jej konfiguracji. Ten typ źródła umożliwia tworzenie kopii zapasowych wielu maszyn. Jest to przydatne, gdy istnieje duża liczba małych (pod względem pojemności dysków wirtualnych) serwerów starszego typu, na przykład powstałych w związku z konsolidacją obciążenia. Dla każdej maszyny zostanie utworzone osobne archiwum.

Tworzenie kopii zapasowej woluminów maszyny wirtualnej przypomina tworzenie kopii zapasowej woluminów komputera fizycznego. Ten typ źródła umożliwia wybranie maszyny, a następnie wybranie dysków/woluminów do utworzenia kopii zapasowej. Jest to przydatne, gdy system operacyjny i aplikacje, na przykład serwer bazy danych, działają na dysku wirtualnym, ale dane, na przykład baza danych, są przechowywane na dysku fizycznym o dużej pojemności dodanym do tej

samej maszyny. Do dysku wirtualnego i magazynu fizycznego można zastosować różne strategie tworzenia kopii zapasowych. Tworzona jest również kopia zapasowa konfiguracji maszyny wirtualnej.

Ograniczenia

Z poziomu hosta nie można utworzyć kopii zapasowej maszyny wirtualnej Hyper-V wykorzystującej co najmniej jeden dysk typu pass-through (dysk fizyczny — lokalny lub SAN-LUN — podłączony do maszyny wirtualnej). Aby utworzyć kopię zapasową takiej maszyny lub jej dysków, należy na niej zainstalować agenta dla systemu Windows lub agenta dla systemu Linux.

Z poziomu hosta nie można utworzyć kopii zapasowej uruchomionej (znajdującej się w trybie online) maszyny wirtualnej ESX/ESXi mającej niezależny dysk lub dysk RDM podłączony w trybie kompatybilności fizycznej. Aby utworzyć kopię zapasową takiej maszyny lub jej dysków, należy ją zatrzymać lub zainstalować na niej agenta dla systemu Windows lub agenta dla systemu Linux.

Kopia zapasowa maszyny wirtualnej a kopia zapasowa komputera fizycznego

Utworzenie kopii zapasowej całej maszyny wirtualnej lub jej woluminów powoduje utworzenie standardowej kopii zapasowej dysku (s. 424). Komponent Acronis Backup & Recovery 10 Agent dla systemu Windows lub Acronis Backup & Recovery 10 Agent dla systemu Linux umożliwia montowanie woluminów, a także odzyskiwanie poszczególnych plików oraz dysków i woluminów z kopii zapasowej na komputer fizyczny.

W podobny sposób dyski i woluminy z kopii zapasowej komputera fizycznego, utworzonej przy użyciu agenta dla systemu Windows albo agenta dla systemu Linux, można odzyskiwać na nową lub istniejącą maszynę wirtualną przy użyciu agenta dla maszyn wirtualnych. Możliwa jest zatem migracja między komputerami fizycznymi a maszynami wirtualnymi.

Systemy operacyjne-goście

Obsługiwane są poniższe systemy operacyjne-goście.

Platforma Microsoft Windows:

- Microsoft Windows 2000
- Microsoft Windows XP
- Microsoft Windows Server 2003
- Microsoft Windows Server 2003 R2
- Microsoft Vista
- Microsoft Windows Server 2008
- Microsoft Windows Server 2008 R2
- Microsoft Windows 7

Platforma Linux

Dyski twarde-goście

Obsługiwane są poniższe konfiguracje dysków wirtualnych.

Styl partycjonowania: główny rekord rozruchowy (MBR).

Typy woluminów: woluminy podstawowe i dynamiczne.

Woluminy dynamiczne (LDM w systemie Windows i LVM w systemie Linux) są obsługiwane w takim samym zakresie jak na komputerach fizycznych. Aby zachować mechanizm LDM/LVM, strukturę LDM/LVM należy utworzyć przed rozpoczęciem odzyskiwania. W tym celu należy uruchomić

docelową maszynę wirtualną przy użyciu nośnika startowego (s. 424) lub odpowiedniego obrazu ISO, a następnie użyć programu Acronis Disk Director Lite w celu rekonstrukcji LDM bądź narzędzi wiersza polecenia systemu Linux w celu rekonstrukcji LVM. Można również odzyskać woluminy dynamiczne jako podstawowe.

Rozwiązywanie problemów

Agent: Agent dla Hyper-V

Problem: Tworzenie kopii zapasowej maszyny wirtualnej kończy się niepowodzeniem z powodu błędu usługi kopiowania woluminów w tle (VSS). Błąd jest widoczny w dzienniku zdarzeń aplikacji (identyfikator zdarzenia = 8193).

Przyczyna: Dzieje się tak ze względu na brak klucza rejestru:

```
HKEY_CLASSES_ROOT\Wow6432Node\CLSID\{F2C2787D-95AB-40D4-942D-298F5F757874}
```

Rozwiązanie: Dodaj klucz do rejestru. W tym celu utwórz i uruchom następujący skrypt (xxx.reg):

```
[HKEY_CLASSES_ROOT\Wow6432Node\CLSID\{F2C2787D-95AB-40D4-942D-298F5F757874}]
@="PSFactoryBuffer"
[HKEY_CLASSES_ROOT\Wow6432Node\CLSID\{F2C2787D-95AB-40D4-942D-
298F5F757874}\InProcServer32]
@=hex(2):25,00,73,00,79,00,73,00,74,00,65,00,6d,00,72,00,6f,00,6f,00,74,00,25,\
  00,5c,00,53,00,79,00,73,00,57,00,4f,00,57,00,36,00,34,00,5c,00,76,00,73,00,\
  73,00,5f,00,70,00,73,00,2e,00,64,00,6c,00,6c,00,00,00
"ThreadingModel"="Both"
```

2.11.1 Jak zainstalować usługi integracyjne Hyper-V

Aby zainstalować usługi integracyjne Hyper-V

1. Uruchom system operacyjny-gościa.
2. Wybierz **Czynność > Włóż dysk instalacyjny usług integracji.**
3. Serwer nawiąże połączenie z obrazem ISO dysku instalacyjnego komputera. Postępuj zgodnie z wyświetlanymi instrukcjami.

2.11.2 Jak zainstalować narzędzia VMware

Aby zainstalować narzędzia VMware:

1. Uruchom klienta infrastruktury VMware/vSphere.
2. Nawiąż połączenie z serwerem ESX.
3. Wybierz maszynę wirtualną i uruchom system operacyjny-gościa.
4. Kliknij komputer prawym przyciskiem myszy i wybierz **Install/Upgrade VMware Tools** (Instaluj/Aktualizuj narzędzia VMware).
5. Postępuj zgodnie z wyświetlanymi instrukcjami.

2.12 Obsługa taśmy

Program Acronis Backup & Recovery 10 obsługuje biblioteki taśm, automatyczne zmieniacze taśm oraz napędy taśmowe SCSI i USB jako urządzenia pamięci. Urządzenie taśmowe może być podłączone lokalnie do komputera zarządzanego (w takim przypadku agent Acronis Backup & Recovery 10

zapisuje i odczytuje taśmy) lub dostępne poprzez węzeł Acronis Backup & Recovery 10 Storage Node (s. 22). Węzły magazynowania umożliwiają w pełni automatyczne działanie bibliotek taśm i automatycznych zmieniaczy taśm (s. 152).

Archiwa kopii zapasowych, które zostały utworzone przy użyciu różnych sposobów dostępu do taśmy, mają odmienne formaty. Taśma zapisana przez węzeł magazynowania nie może zostać odczytana przez agenta.

Nośniki startowe oparte na systemie Linux i środowisku PE umożliwiają tworzenie i odzyskiwanie kopii zapasowych przy użyciu dostępu lokalnego, jak i poprzez węzeł magazynowania. Kopie zapasowe utworzone przy użyciu nośnika startowego mogą być odzyskiwane za pomocą agenta Acronis Backup & Recovery 10 uruchomionego w systemie operacyjnym.

2.12.1 Tabela kompatybilności taśm

W poniższej tabeli przedstawiono możliwości odczytania taśm zapisanych przez programy z serii Acronis True Image Echo i Acronis True Image 9.1 w programie Acronis Backup & Recovery 10. Tabela przedstawia również kompatybilność taśm zapisanych przez różne komponenty programu Acronis Backup & Recovery 10.

			...można odczytać przy użyciu urządzenia taśmowego podłączonego do komputera zawierającego...			
			Nośnik startowy ABR10	Agent dla systemu Windows ABR10	Agent dla systemu Linux ABR10	Węzeł magazynowania ABR10
Taśmę zapisaną na lokalnie podłączonym urządzeniu taśmowym (napędzie taśmowym lub w bibliotece taśm) przez...	Nośnik startowy	ATIE 9.1	+	+	+	+
		ATIE 9.5	+	+	+	+
		ATIE 9.7	+	+	+	+
		ABR10	+	+	+	+
	Agent dla systemu Windows	ATIE 9.1	+	+	+	+
		ATIE 9.5	—	—	—	+
		ATIE 9.7	—	—	—	+
		ABR10	+	+	+	+
	Agent dla systemu Linux	ATIE 9.1	+	+	+	+
		ATIE 9.5	+	+	+	+
		ATIE 9.7	+	+	+	+
		ABR10	+	+	+	+
Taśma zapisana na urządzeniu taśmowym przez...	Backup Server	ATIE 9.1	+	+	+	+
		ATIE 9.5	—	—	—	+
		ATIE 9.7	—	—	—	+

	Storage Node	ABR10	—	—	—	+

2.12.2 Używanie jednego napędu taśm

Napędu taśmowego podłączonego lokalnie do zarządzanego komputera można używać jako urządzenia pamięci masowej w lokalnych planach tworzenia kopii zapasowych. Funkcjonalność podłączonego lokalnie układu automatycznego ładowania lub biblioteki jest ograniczona do funkcji zwykłego napędu taśmowego. Oznacza to, że program może pracować tylko z aktualnie zamontowaną taśmą i taśmy należy montować ręcznie.

Tworzenie kopii zapasowej na lokalnie podłączonym urządzeniu taśmowym

Podczas tworzenia planu tworzenia kopii zapasowych jako miejsce docelowe kopii zapasowych można wybrać podłączone lokalnie urządzenie taśmowe. Podczas tworzenia kopii zapasowej na taśmie nazwa archiwum nie jest wymagana.

Archiwum może zajmować kilka taśm, ale może zawierać tylko jedną pełną kopię zapasową i nieograniczoną liczbę kopii przyrostowych. Przy każdym utworzeniu pełnej kopii zapasowej rozpoczyna się od nowej taśmy i tworzy nowe archiwum. Po zapełnieniu taśmy program wyświetla okno dialogowe z prośbą o włożenie nowej taśmy.

Zawartość taśmy zostanie zastąpiona po wyświetleniu monitu. Wyświetlanie monitów można wyłączyć, zobacz Ustawienia dodatkowe (s. 132).

Obejście

Aby zapisać kilka archiwów na jednej taśmie, na przykład utworzyć oddzielne kopie zapasowe woluminów C i D, dla drugiego woluminu należy wybrać przyrostową kopię zapasową zamiast pełnej kopii. W innych sytuacjach w celu uwzględnienia zmian w zapisanym wcześniej archiwum jest używana przyrostowa kopia zapasowa.

Mogą występować krótkie pauzy potrzebne na przewinięcie taśmy. Stara taśma lub taśma o niskiej jakości, a także zabrudzenia głowicy magnetycznej mogą powodować powstawanie przerw trwających nawet kilka minut.

Ograniczenia

1. Tworzenie kilku kopii zapasowych w jednym archiwum nie jest obsługiwane.
2. Nie można odzyskiwać poszczególnych plików z kopii zapasowej dysku.
3. Podczas czyszczenia nie można usuwać kopii zapasowych z taśmy ani ręcznie, ani automatycznie. Reguły przechowywania i schematy tworzenia kopii zapasowych używające automatycznego czyszczenia (GFS, Wieża Hanoi) są niedostępne w interfejsie graficznym podczas tworzenia kopii na podłączonych lokalnie taśmach.
4. Na urządzeniach taśmowych nie można tworzyć skarbców osobistych.
5. Ponieważ w przypadku kopii zapasowej zapisanej na taśmie nie można określić, czy obejmuje ona system operacyjny, podczas odzyskiwania dysków i woluminów zaleca się użycie funkcji Acronis Universal Restore (s. 430), nawet gdy jest odzyskiwany wolumin systemu Linux lub systemu innego niż Windows.
6. Funkcja Acronis Active Restore (s. 418) jest niedostępna w przypadku odzyskiwania z taśmy.

Odzyskiwanie z lokalnie podłączonego urządzenia taśmowego

Przed utworzeniem zadania odzyskiwania należy zamontować taśmę zawierającą odpowiednią kopię zapasową. Podczas tworzenia zadania odzyskiwania należy z listy dostępnych lokalizacji wybrać

urządzenie taśmowe, a następnie kopię zapasową. Po rozpoczęciu odzyskiwania będą wyświetlane monity o zamontowanie kolejnych taśm, jeśli będą one wymagane w procesie odzyskiwania.

2.13 Obsługa SNMP

Obiekty SNMP

Program Acronis Backup & Recovery 10 udostępnia następujące obiekty protokołu Simple Network Management Protocol (SNMP) aplikacjom zarządzającym SNMP:

- Typ zdarzenia

  Identyfikator obiektu (OID): 1.3.6.1.4.1.24769.100.200.1.0

  Składnia: OctetString

  Możliwe są następujące wartości: „Informacja”, „Ostrzeżenie”, „Błąd” lub „Nieznane”. Wartość „Nieznane” jest wysyłana tylko w wiadomości próbnej.
- Tekstowy opis zdarzenia

  Identyfikator obiektu (OID): 1.3.6.1.4.1.24769.100.200.2.0

  Składnia: OctetString

  Wartość zawiera opis tekstowy zdarzenia (wygląda identycznie, jak wiadomości publikowane przez program Acronis Backup & Recovery 10 w jego dzienniku).

Przykłady wartości varbind:

1.3.6.1.4.1.24769.100.200.1.0:Informacja

1.3.6.1.4.1.24769.100.200.2.0:I0064000B

Obsługiwane operacje

Program Acronis Backup & Recovery 10 **obsługuje tylko operacje TRAP**. Nie jest możliwe zarządzanie programem Acronis Backup & Recovery 10 przy użyciu żądań GET- i SET-. Oznacza to, że należy używać odbiornika SNMP Trap w celu odbierania wiadomości TRAP.

Informacje na temat bazy informacji zarządzania (MIB)

Plik MIB **acronis-abr.mib** znajduje się w katalogu instalacyjnym programu Acronis Backup & Recovery 10. Domyślnie: %ProgramFiles%\Acronis\BackupAndRecovery w systemie Windows i /usr/lib/Acronis/BackupAndRecovery w systemie Linux.

Ten plik można odczytać przy użyciu przeglądarki plików MIB lub prostego edytora tekstowego, takiego jak Notatnik lub vi.

Informacje na temat wiadomości próbnej

Podczas konfigurowania powiadomień SNMP możesz wysłać wiadomość próbną, aby sprawdzić, czy ustawienia są poprawne.

Parametry wiadomości próbnej są następujące:

- Typ zdarzenia

  OID: 1.3.6.1.4.1.24769.100.200.1.0

  Wartość: „Nieznane”
- Tekstowy opis zdarzenia

  OID: 1.3.6.1.4.1.24769.100.200.2.0

Wartość: „?00000000”

2.14 Własne technologie Acronis

W tej sekcji opisano technologie odziedziczone przez program Acronis Backup & Recovery 10 z rodzin produktów Acronis True Image Echo i Acronis True Image 9.1.

2.14.1 Strefa Acronis Secure Zone

Strefa Acronis Secure Zone to bezpieczna partycja, która umożliwia przechowywanie archiwów kopii zapasowych na dysku zarządzanego komputera. Dzięki temu dysk można odzyskać na tym samym dysku, na którym znajduje się jego kopia zapasowa.

Dostęp do tej strefy mogą uzyskać pewne aplikacje systemu Windows, takie jak narzędzia do zarządzania dyskami firmy Acronis.

W przypadku fizycznej awarii dysku strefa i znajdujące się w niej archiwa zostaną utracone. Z tego powodu strefa Acronis Secure Zone nie powinna być jedyną lokalizacją do przechowywania kopii zapasowych. W infrastrukturze przedsiębiorstwa strefa Acronis Secure Zone może służyć jako pośrednia lokalizacja kopii zapasowych, używana w przypadku, gdy normalna lokalizacja jest tymczasowo niedostępna albo podłączona poprzez powolny lub obciążony kanał przesyłowy.

Korzyści

Strefa Acronis Secure Zone:

- umożliwia odzyskanie zawartości dysku na ten sam dysk, na którym znajduje się jego kopia zapasowa;
- tania i przydatna metoda ochrona danych przed nieprawidłowym działaniem oprogramowania, atakiem wirusów, błędem operatora;
- ponieważ służy jako wewnętrzna lokalizacja archiwum, eliminuje potrzebę użycia dodatkowego nośnika lub połączenia sieciowego w celu utworzenia kopii zapasowej lub odzyskania danych. Jest to szczególnie przydatne dla użytkowników urządzeń mobilnych;
- Może służyć jako lokalizacja podstawowa w przypadku tworzenia kopii zapasowej w dwóch miejscach docelowych (s. 128).

Ograniczenia

- Nie można organizować strefy na dysku dynamicznym ani na dysku, na którym jest stosowany styl partycjonowania GPT.

Zarządzanie strefą Acronis Secure Zone

Strefa Acronis Secure Zone jest obsługiwana jako skarbiec osobisty (s. 428). Po utworzeniu na komputerze zarządzanym strefa jest zawsze obecna na liście **Skarbce osobiste**. Strefa Acronis Secure Zone może być używana w scentralizowanych planach tworzenia kopii zapasowych (s. 427), a także w planach lokalnych (s. 424).

Dotychczasowym użytkownikom strefy Acronis Secure Zone zwracamy uwagę na poważne zmiany w jej działaniu. Strefa nie wykonuje już automatycznego czyszczenia, tzn. usuwania starych archiwów. Aby utworzyć kopię zapasową strefy lub ręcznie usunąć nieaktualne kopie zapasowe przy użyciu funkcji zarządzania archiwami, należy użyć schematów tworzenia kopii zapasowych z automatycznym czyszczeniem.

Nowy sposób działania strefy Acronis Secure Zone umożliwia:

- wyświetlanie listy archiwów znajdujących się w strefie i kopii zapasowych zawartych w każdym archiwum;
- sprawdzanie zawartości kopii zapasowej;
- zamontowanie kopii zapasowej dysku w celu skopiowania plików z kopii zapasowej na dysk fizyczny;
- bezpieczne usunięcie archiwów oraz kopii zapasowych z archiwów.

Więcej informacji na temat operacji dostępnych w strefie Acronis Secure Zone zawiera sekcja Skarbce osobiste (s. 177).

Aktualizacja z produktu Acronis True Image Echo

Podczas aktualizacji z programu Acronis True Image Echo do programu Acronis Backup & Recovery 10 strefa Acronis Secure Zone zachowa archiwa utworzone za pomocą programu Echo Strefa pojawi się na liście skarbców osobistych, a stare archiwa będą dostępne w celu odzyskiwania.

2.14.2 Acronis Startup Recovery Manager

Na dysku systemowym można umieścić modyfikację agenta startowego (s. 418) i skonfigurować ją tak, aby uruchamiała się podczas rozruchu po naciśnięciu klawisza F11. Dzięki temu do uruchamiania ratunkowego narzędzia startowego nie trzeba używać nośnika ratunkowego ani połączenia sieciowego. Nazwa handlowa tej funkcji brzmi „Acronis Startup Recovery Manager”.

Acronis Startup Recovery Manager jest szczególnie przydatny dla użytkowników urządzeń przenośnych. W razie awarii należy ponownie uruchomić komputer, nacisnąć klawisz F11 po wyświetleniu monitu „Naciśnij klawisz F11, aby uruchomić Acronis Startup Recovery Manager...” oraz odzyskać dane w taki sam sposób jak ze zwykłego nośnika startowego. Ponadto podczas podróży można używać funkcji Acronis Startup Recovery Manager do tworzenia kopii zapasowych.

Na komputerach z zainstalowanym programem ładującym GRUB użytkownik wybiera funkcję Acronis Startup Recovery Manager z menu startowego, a nie przez naciśnięcie klawisza F11.

Aktywacja i dezaktywacja funkcji Acronis Startup Recovery Manager

Operacja umożliwiająca korzystanie z funkcji Acronis Startup Recovery Manager nosi nazwę „aktywacji”. Aby aktywować program Acronis Startup Recovery Manager, z menu programu wybierz **Czynności > Aktywuj program Acronis Startup Recovery Manager**.

Program Acronis Startup Recovery Manager można aktywować lub dezaktywować w dowolnej chwili w menu **Narzędzia**. Dezaktywacja powoduje wyłączenie monitu „Naciśnij klawisz F11, aby uruchomić Acronis Startup Recovery Manager” wyświetlanego w czasie rozruchu (lub usunięcie odpowiedniego wpisu z menu startowego programu GRUB). Oznacza to, że w przypadku nieudanego uruchamiania systemu potrzebny będzie nośnik startowy.

Ograniczenie

Aktywacja programu Acronis Startup Recovery Manager wymaga ponownej aktywacji programów ładujących innych firm.

Aktualizacja z programu Acronis True Image Echo

Po aktualizacji programu Acronis True Image Echo do programu Acronis Backup & Recovery 10, program Acronis Startup Recovery Manager jest wyświetlany jako nieaktywny, niezależnie od statusu

przed aktualizacją. W dowolnym momencie można ponownie aktywować program Acronis Startup Recovery Manager.

2.14.3 Universal Restore (Acronis Backup & Recovery 10 Universal Restore)

Acronis Backup & Recovery 10 Universal Restore to zastrzeżona technologia firmy Acronis, która ułatwia odzyskiwanie i uruchamianie systemu Windows na sprzęcie o innej konfiguracji lub na maszynie wirtualnej. Moduł Universal Restore niweluje różnice między urządzeniami istotnymi dla uruchamiania systemu operacyjnego, takimi jak kontrolery pamięci, płyta główna i chipset.

Przeznaczenie modułu Acronis Backup & Recovery 10 Universal Restore

Zawartość systemu zapisaną w kopii zapasowej (obrazie) dysku można w prosty sposób odzyskać do tego samego systemu lub na identyczny sprzęt. Jednak w przypadku zmiany płyty głównej lub użycia innej wersji procesora, co zdarza się często w przypadku awarii sprzętu, uruchomienie odzyskanego systemu może okazać się niewykonalne. Próba przeniesienia systemu na nowy, mocniejszy komputer zazwyczaj zakończy się podobnie, ponieważ nowy sprzęt będzie niekompatybilny z większością newralgicznych sterowników zawartych w obrazie.

Problemu tego nie rozwiąże użycie narzędzia przygotowywania systemu firmy Microsoft (Sysprep), ponieważ narzędzie to umożliwia instalację tylko sterowników urządzeń Plug and Play (kart dźwiękowych, kart sieciowych, kart graficznych itp.). Systemowe sterowniki warstwy abstrakcji sprzętu (HAL) i urządzeń pamięci masowej muszą być identyczne na komputerze źródłowym i docelowym (zobacz artykuły 302577 i 216915 w bazie wiedzy Microsoft Knowledge Base).

Technologia Universal Restore zapewnia skuteczne rozwiązanie w zakresie niezależnego sprzętowo odzyskiwania systemu dzięki zastąpieniu najważniejszych sterowników warstwy abstrakcji sprzętu (HAL) i urządzeń pamięci masowej.

Zastosowania technologii Universal Restore:

1. Błyskawiczne odzyskiwanie uszkodzonego systemu na innym sprzęcie.
2. Niezależne sprzętowo klonowanie i wdrażanie systemów operacyjnych.
3. Migracja komputerów typu „fizyczny na fizyczny”, „fizyczny na wirtualny” oraz „wirtualny na fizyczny”.

Zasady działania technologii Universal Restore

1. Automatyczny wybór sterowników HAL i pamięci masowej.

   Moduł Universal Restore wyszukuje sterowniki w określonych folderach sieciowych, na nośnikach wymiennych i w domyślnych folderach przechowywania sterowników w odzyskiwanym systemie. Następnie moduł analizuje poziom kompatybilności wszystkich znalezionych sterowników oraz instaluje sterowniki HAL i pamięci masowej, które lepiej pasują do sprzętu docelowego. Universal Restore wyszukuje również sterowniki kart sieciowych i przekazuje je do systemu operacyjnego, który instaluje te sterowniki automatycznie po pierwszym uruchomieniu.

   *Domyślny folder przechowywania sterowników w systemie Windows jest określony przez wartość **DevicePath**, którą można znaleźć w kluczu rejestru **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion**. Zwykle jest to folder WINDOWS/inf.*

2. Ręczny wybór sterownika urządzenia pamięci masowej.

Jeśli komputer docelowy zawiera określony kontroler pamięci masowej dla dysku twardego (na przykład SCSI, RAID lub Fibre Channel), odpowiedni sterownik można zainstalować ręcznie, pomijając procedurę automatycznego wyszukiwania i instalowania sterowników.

3. Instalowanie sterowników urządzeń Plug and Play.

   Moduł Universal Restore wykorzystuje wbudowany proces wykrywania i konfigurowania urządzeń Plug and Play w celu zniwelowania różnic między urządzeniami, które nie mają krytycznego znaczenia dla uruchomienia systemu, takimi jak karty graficzne, dźwiękowe i USB. System Windows przejmuje kontrolę nad tym procesem w fazie logowania, a jeśli jakiś nowy sprzęt nie zostanie wykryty, można później ręcznie zainstalować odpowiednie sterowniki.

Universal Restore i Microsoft Sysprep

Moduł Universal Restore nie jest narzędziem służącym do przygotowania systemu. Można go zastosować do dowolnego obrazu systemu Windows utworzonego przez programy firmy Acronis, w tym do obrazów systemów przygotowanych za pomocą narzędzia przygotowywania systemu firmy Microsoft (Sysprep). Poniżej przedstawiono przykład użycia obu narzędzi w tym samym systemie.

Moduł Universal Restore nie usuwa identyfikatora zabezpieczeń (SID) ani ustawień profili użytkowników, aby umożliwić natychmiastowe uruchomienie odzyskanego systemu bez ponownego dołączania do domeny oraz ponownego mapowania sieciowych profili użytkowników. Jeśli jest planowana zmiana powyższych ustawień w odzyskanym systemie, można przygotować system przy użyciu narzędzia Sysprep, utworzyć jego obraz, a następnie odzyskać go w razie potrzeby za pomocą modułu Universal Restore.

Ograniczenia

Moduł Universal Restore jest niedostępny w następujących przypadkach:

- uruchamianie komputera za pomocą programu Acronis Startup Recovery Manager (przez naciśnięcie klawisza F11),
- umiejscowienie odzyskiwanego obrazu w strefie Acronis Secure Zone,
- używanie funkcji Acronis Active Restore,

ponieważ są to funkcje przeznaczone głównie do natychmiastowego odzyskiwania danych na tym samym komputerze.

Moduł Universal Restore jest niedostępny w przypadku odzyskiwania systemu Linux.

Uzyskiwanie modułu Universal Restore

Moduł Universal Restore jest dostępny bezpłatnie z programami Acronis Backup & Recovery 10 Advanced Server SBS Edition oraz Acronis Backup & Recovery 10 Advanced Server Virtual Edition.

Do innych wersji programu można go zakupić osobno z odrębną licencją, a instaluje się go jako oddzielną funkcję przy użyciu pliku instalatora. Aby nowo zainstalowany dodatek działał w środowisku startowym, należy ponownie utworzyć nośniki startowe.

2.14.4 Acronis Active Restore

Active Restore to zastrzeżona technologia firmy Acronis, która umożliwia przywrócenie sprawności systemu niezwłocznie po rozpoczęciu jego odzyskiwania.

Użytkownicy, którzy znają już produkt Acronis Recovery for Microsoft Exchange, mogą zauważyć, że używa on funkcji Active Restore w celu zapewnienia dostępności magazynu informacji programu Exchange niezwłocznie po uruchomieniu odzyskiwania. Chociaż funkcja ta jest oparta na identycznej

technologii, odzyskiwanie magazynu informacji odbywa się w inny sposób niż odzyskiwanie systemu operacyjnego, które opisano w tej sekcji.

Obsługiwane systemy operacyjne

Funkcja Acronis Active Restore jest dostępna przy odzyskiwaniu systemu Windows począwszy od wersji Windows 2000.

Ograniczenie

Jedyną obsługiwaną lokalizacją archiwum jest dysk lokalny, a dokładniej — dowolne urządzenie dostępne z poziomu systemu BIOS komputera. Może to być strefa Acronis Secure Zone, dysk twardy USB, dysk flash lub dowolny wewnętrzny dysk twardy.

Sposób działania

Podczas konfigurowania operacji odzyskiwania należy wybrać dyski lub woluminy do odzyskania z kopii zapasowej. Program Acronis Backup & Recovery 10 skanuje wybrane dyski lub woluminy w kopii zapasowej. Jeśli zostanie znaleziony obsługiwany system operacyjny, opcja Acronis Active Restore stanie się dostępna.

Jeśli opcja nie zostanie włączona, odzyskiwanie systemu będzie wykonywane w zwykły sposób, a komputer rozpocznie działanie po zakończeniu odzyskiwania.

W przypadku włączenia tej opcji zostanie ustawiona poniższa kolejność czynności do wykonania.

Po rozpoczęciu odzyskiwania systemu następuje uruchomienie systemu operacyjnego z kopii zapasowej. Komputer odzyskuje sprawność i może udostępniać niezbędne usługi. Najwyższy priorytet odzyskiwania mają dane umożliwiające obsługę żądań przychodzących. Reszta danych jest odzyskiwana w tle.

Ponieważ żądania są obsługiwane równocześnie z procesem odzyskiwania, system może działać wolniej, nawet jeśli priorytet odzyskiwania w opcjach odzyskiwania został ustawiony na **Niski**. W ten sposób czas przestoju systemu jest ograniczany do minimum kosztem tymczasowego obniżenia wydajności.

Scenariusze użycia

1. Czas bezawaryjnej pracy systemu stanowi jedno z kryteriów wydajności.

   Przykłady: usługi online dla klientów, sklepy internetowe, stanowiska do głosowania.

2. Przechowywane dane zajmują znacznie więcej miejsca niż system.

   Niektóre komputery służą jako urządzenia magazynujące. W takim przypadku system operacyjny zajmuje niewiele miejsca, a pozostała część dysku jest przeznaczona na dane, na przykład filmy, utwory muzyczne lub inne pliki multimedialne. Niektóre woluminy przeznaczone na dane mogą być bardzo duże w porównaniu z systemem, przez co praktycznie cały czas odzyskiwania przypada na odzyskanie plików, które mogą być potrzebne w dużo bardziej odległej przyszłości.

   Jeśli zostanie wybrana opcja Acronis Active Restore, system wznowi działanie w bardzo krótkim czasie. Użytkownicy będą mogli otwierać niezbędne pliki z magazynu, podczas gdy pozostałe pliki, niewymagane natychmiast, będą odzyskiwane w tle.

   Przykłady: magazyn kolekcji filmów, magazyn kolekcji muzycznej, magazyn multimediów.

Sposób korzystania

1. Utwórz kopię zapasową dysku lub woluminu systemowego w lokalizacji dostępnej z poziomu systemu BIOS komputera. Może to być strefa Acronis Secure Zone, dysk twardy USB, dysk flash lub dowolny wewnętrzny dysk twardy.

Jeśli system operacyjny i jego program ładujący znajdują się na różnych woluminach, w kopii zapasowej należy zawsze uwzględnić oba woluminy. Woluminy muszą być również odzyskiwane wspólnie, gdyż w przeciwnym razie istnieje duże ryzyko, że system operacyjny nie uruchomi się.

2. Utwórz nośnik startowy.
3. Jeśli wystąpi awaria systemu, uruchom komputer przy użyciu nośnika startowego. Uruchom konsolę i połącz się z agentem startowym.
4. Skonfiguruj odzyskiwanie systemu: wybierz dysk lub wolumin systemowy, a następnie zaznacz pole wyboru **Użyj funkcji Acronis Active Restore**.

   Na potrzeby rozruchu i późniejszego odzyskiwania funkcja Acronis Active Restore wybierze pierwszy system operacyjny znaleziony podczas skanowania kopii zapasowej. Aby wyniki były przewidywalne, przy użyciu funkcji Active Restore nie należy odzyskiwać więcej niż jednego systemu operacyjnego. W przypadku odzyskiwania danych na komputerze z wieloma systemami operacyjnymi należy wybierać jednocześnie tylko jeden wolumin systemowy i jeden wolumin startowy.
5. Po rozpoczęciu odzyskiwania systemu następuje uruchomienie systemu operacyjnego z kopii zapasowej. Na pasku zadań pojawia się ikona funkcji Acronis Active Restore. Komputer odzyskuje sprawność i może udostępniać niezbędne usługi. Bezpośredni użytkownik widzi drzewo dysków i ikony oraz może otwierać pliki lub uruchamiać aplikacje, nawet jeśli nie zostały one jeszcze odzyskane.

   Sterowniki Acronis Active Restore przechwytują zapytania systemowe i ustawiają najwyższy priorytet odzyskiwania plików, które są wymagane do obsługi żądań przychodzących. Podczas tego odzyskiwania „w locie” trwający proces odzyskiwania zostaje przeniesiony w tło.

   Nie należy wyłączać ani ponownie uruchamiać komputera aż do zakończenia odzyskiwania. Jeśli wyłączysz komputer, wszystkie zmiany dokonane w systemie od momentu ostatniego uruchomienia zostaną utracone. System nie zostanie odzyskany (nawet częściowo). W takim przypadku jedynym możliwym rozwiązaniem będzie ponowne rozpoczęcie procesu odzyskiwania z nośnika startowego.
6. Odzyskiwanie w tle jest kontynuowane do momentu odzyskania wszystkich wybranych woluminów, utworzenia wpisu dziennika i zniknięcia ikony Acronis Active Restore z paska zadań.

2.15 Opis zarządzania scentralizowanego

Ta sekcja zawiera omówienie scentralizowanej ochrony danych przy użyciu programu Acronis Backup & Recovery 10. Przed lekturą tej sekcji należy zapoznać się z metodami ochrony danych na jednym komputerze (s. 30).

2.15.1 Podstawowe pojęcia

Stosowanie zasad tworzenia kopii zapasowych i śledzenie ich wykonywania

Aby chronić dane na komputerze, należy zainstalować na nim agenta (s. 418) lub kilka agentów dla różnych typów danych, które mają być chronione. Można podłączyć konsolę do komputera i utworzyć plan tworzenia kopii zapasowych (s. 425) lub kilka takich planów.

Co jednak zrobić w przypadku konieczności zarządzania setkami komputerów? Utworzenie planu tworzenia kopii zapasowych na każdym komputerze wymaga czasu, nawet jeśli plany będą podobne, gdy na przykład trzeba utworzyć kopię zapasową dysku systemowego i dokumentów użytkowników. Również śledzenie wykonywania planów na każdym komputerze zajmuje dużo czasu.

Aby uzyskać możliwość propagowania operacji zarządzania do wielu komputerów, należy zainstalować serwer Acronis Backup & Recovery 10 Management Server (s. 427) i zarejestrować (s.

427) komputery na serwerze. Następnie można utworzyć grupy komputerów, co umożliwi jednoczesne zarządzanie wieloma komputerami. Wszystkie komputery lub ich wybraną część można chronić, tworząc wspólny plan tworzenia kopii zapasowych, który jest nazywany zasadami tworzenia kopii zapasowych (s. 433).

Po zastosowaniu zasad do grupy komputerów serwer zarządzania wdraża zasady na wszystkich komputerach. Na każdym komputerze agenty znajdują elementy wymagające utworzenia kopii zapasowych i tworzą odpowiednie scentralizowane plany tworzenia kopii zapasowych (s. 427). Stan zasad można monitorować na pojedynczym ekranie, przechodząc w razie potrzeby do poszczególnych komputerów, planów lub zadań, aby sprawdzić ich stan i wpisy dziennika. Serwer zarządzania pozwala także na monitorowanie zainicjowanych lokalnie działań agenta i zarządzanie nimi.

Ponieważ konsolę podłącza się do serwera zarządzania, a nie do poszczególnych komputerów, a wszystkie operacje zarządzania wykonuje się za pośrednictwem jednostki zarządzania centralnego, ten sposób zarządzania nazywa się zarządzaniem scentralizowanym (s. 432).

Zarządzanie scentralizowane nie wyklucza bezpośredniego zarządzania (s. 432) każdym komputerem. Konsolę można podłączyć do poszczególnych komputerów w celu wykonania dowolnych operacji zarządzania bezpośredniego. Zarządzanie scentralizowanymi planami tworzenia kopii zapasowych jest jednak możliwe tylko z poziomu serwera zarządzania, ponieważ dobrze przemyślane zasady działają automatycznie i rzadko wymagają interwencji człowieka.

Korzystając z serwera zarządzania, można utworzyć jedno lub więcej scentralizowanych archiwów pamięci masowej (skarbców centralnych (s. 428)), które będą współużytkowane przez zarejestrowane komputery. Skarbiec centralny może być używany przez dowolne zasady tworzenia kopii zapasowych, a także przez dowolny plan tworzenia kopii zapasowych utworzony na zarejestrowanych komputerach przy użyciu funkcji zarządzania bezpośredniego.

Organizowanie zarządzanego archiwum pamięci masowej

Jaka powinna być pojemność skarbca centralnego? Czy przesyłanie dużych kopii zapasowych do skarbca spowoduje przeciążenie sieci? Czy kopia zapasowa serwera produkcyjnego w trybie online wpłynie na jego wydajność? Aby scentralizowane tworzenie kopii zapasowych nie spowalniało procesów biznesowych w firmie, a także aby zminimalizować ilość zasobów wymaganych do ochrony danych, należy zainstalować węzeł magazynowania Acronis Backup & Recovery 10 Storage Node (s. 430) i skonfigurować go do zarządzania skarbcem centralnym lub wieloma takimi skarbcami. Skarbce tego typu nazywa się skarbcami zarządzanymi (s. 428).

Węzeł magazynowania pomaga agentowi deduplikować (s. 420) kopie zapasowe przed przesłaniem ich do skarbców zarządzanych, a także deduplikuje kopie zapasowe już zapisane w skarbcach. Deduplikacja zmniejsza obciążenie powodowane tworzeniem kopii zapasowych oraz ilość zajmowanego miejsca. Węzeł magazynowania wykonuje również operacje na archiwach (takie jak sprawdzanie poprawności i czyszczenie), które w innym przypadku są wykonywane przez agenta. Pozwala to wyeliminować niepotrzebne obciążenie z zarządzanych komputerów. Nie można też zapominać, że węzeł Acronis Backup & Recovery 10 Storage Node umożliwia użycie biblioteki taśm jako skarbca centralnego do przechowywania archiwów kopii zapasowych.

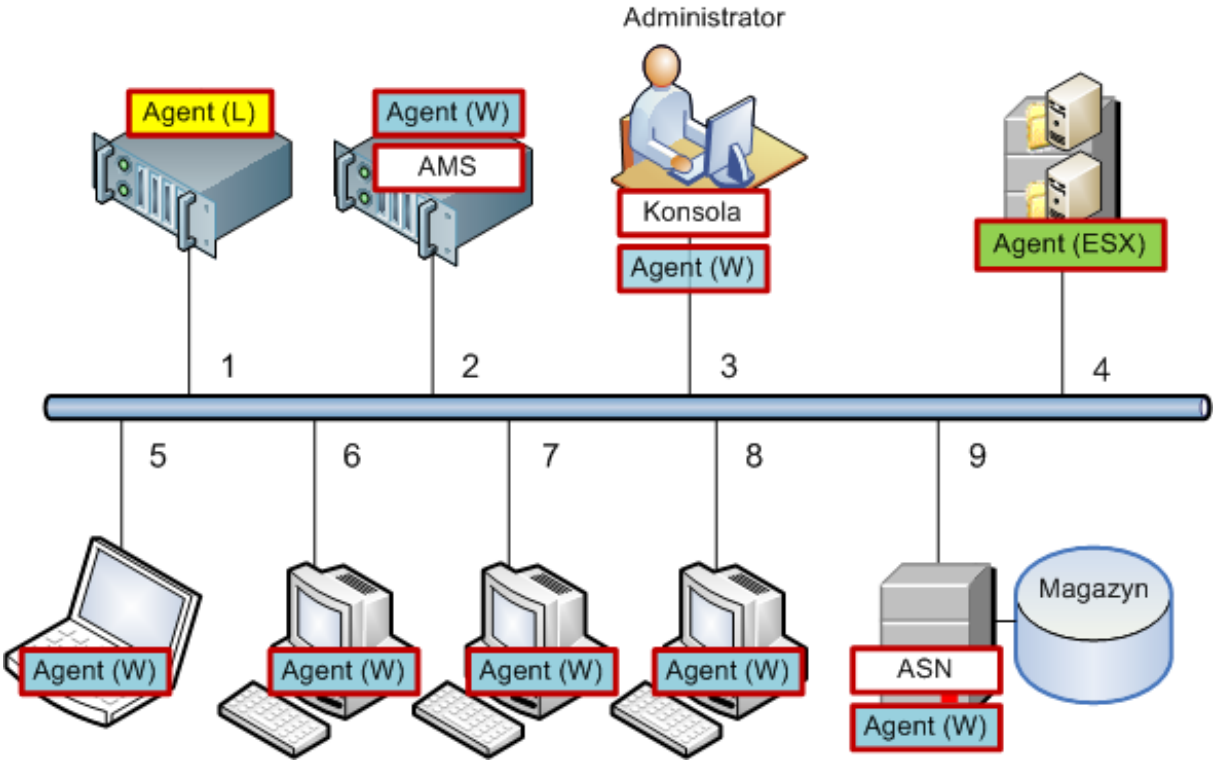
Można skonfigurować wiele węzłów magazynowania, z których każdy zarządza wieloma skarbcami, a sterowanie takimi węzłami odbywa się z poziomu serwera zarządzania Acronis Backup & Recovery 10 Management Server.

Szczegółowe informacje na temat węzłów magazynowania znajdują się w sekcji Węzeł Acronis Backup & Recovery 10 Storage Node (s. 22).

2.15.2 Konfigurowanie scentralizowanej ochrony danych w sieci heterogenicznej

Załóżmy, że infrastruktura sieci obejmuje serwery (1, 2, 9) oraz stacje robocze (3, 5–8), działające w systemach Windows i Linux. Jest jeszcze serwer VMware ESX (4), który jest hostem dwóch systemów-gości.

Ochrony wymagają: każdy z serwerów w całości, dane użytkowników na stacjach roboczych i maszyny wirtualne. Ważna jest możliwość śledzenia stanu ochrony danych, wyeliminowanie duplikatów z archiwów kopii zapasowych oraz terminowe usuwanie przestarzałych kopii zapasowych. Cele te można osiągnąć przez regularne tworzenie kopii zapasowych żądanych elementów danych w skarbcu centralnym z aktywną funkcją deduplikacji.



Konfigurowanie infrastruktury Acronis

1. Zainstaluj konsolę zarządzania Acronis Backup & Recovery 10 Management Console **[Konsola]** na preferowanym komputerze **(3)**. Konsola umożliwia dostęp do pozostałych komponentów Acronis i zarządzanie nimi przy użyciu graficznego interfejsu użytkownika.
2. Zainstaluj serwer zarządzania Acronis Backup & Recovery 10 Management Server **[AMS]** na jednym z serwerów Windows **(2)**. Serwer zarządzania to pojedynczy punkt wejścia do infrastruktury Acronis.
3. Zainstaluj agenta programu Acronis Backup & Recovery 10 na każdym komputerze, którego dyski, woluminy i pliki będą uwzględniane w kopiach zapasowych.
   - **Agent (W)** — Agent dla systemu Windows
   - **Agent (L)** — Agent dla systemu Linux

   Podczas instalowania agentów zarejestruj każdy komputer na serwerze zarządzania. W tym celu wprowadź nazwę lub adres IP serwera oraz poświadczenia administratora serwera

w odpowiednim oknie kreatora instalacji. Ewentualnie komputery do serwera zarządzania możesz dodać później, używając ich nazw lub adresów IP.

4. Zainstaluj komponent Acronis Backup & Recovery 10 Agent for ESX **[Agent (ESX)]** na serwerze ESX **(4)** w celu tworzenia kopii zapasowych maszyn wirtualnych z poziomu hosta. Agent jest dostarczany jako urządzenie wirtualne.
5. Zainstaluj węzeł magazynowania Acronis Backup & Recovery 10 Storage Node **[ASN]** na jednym z serwerów Windows **(9)**. Węzeł magazynowania umożliwia zorganizowanie infrastruktury do przechowywania archiwów kopii zapasowych oraz korzystanie z funkcji deduplikacji. Jeśli host ma wystarczające możliwości, węzeł można zainstalować razem z serwerem zarządzania.

   Podczas instalacji węzła magazynowania zarejestruj go na serwerze zarządzania w taki sam sposób jak agenty.

Wskazówki dotyczące instalacji

- Komponenty AMS i ASN można również zainstalować w systemie operacyjnym stacji roboczej.
- W sieci może znajdować się wiele węzłów magazynowania. Każdy z węzłów może zarządzać maksymalnie 20 lokalnymi lub zdalnymi skarbcami.
- W ramach jednej procedury instalacji na komputerze można zainstalować wiele komponentów programu Acronis Backup & Recovery 10.
- W domenie Active Directory można wdrożyć komponenty przy użyciu zasad grupy.

Konfigurowanie węzła magazynowania

Przed użyciem węzła magazynowania należy sprawdzić, czy wszyscy użytkownicy, którzy będą tworzyć kopie zapasowe w skarbcach węzła, mają w tym węźle konta systemu Windows.

- Jeśli węzeł należy do domeny Active Directory, wszyscy użytkownicy domeny będą mogli tworzyć w węźle kopie zapasowe, natomiast wszyscy administratorzy staną się administratorami węzła.
- W grupie roboczej utwórz konto lokalne dla każdego użytkownika, który będzie wykonywał kopie zapasowe w węźle. Członkowie grupy administratorów staną się administratorami węzła. W razie potrzeby można będzie później dodać kolejne konta.

1. Uruchom konsolę i połącz się z serwerem zarządzania.
2. Utwórz skarbiec zarządzany zgodnie z opisem w sekcji Operacje na skarbcach centralnych (s. 147). Podczas tworzenia skarbca zarządzanego włącz funkcję deduplikacji.

Konfigurowanie grup i zasad

Szczegółowe objaśnienia na temat tego, kiedy i dlaczego należy organizować grupy komputerów, znajdują się w sekcji Grupowanie zarejestrowanych komputerów (s. 70). W tym miejscu przedstawiono wybrane scenariusze możliwe w wyżej wspomnianej implementacji programu Acronis Backup & Recovery 10.

Ochrona serwerów

Najprawdopodobniej będziesz tworzyć osobne plany tworzenia kopii zapasowych na każdym z serwerów w zależności od ich roli. Przynajmniej jeden raz należy jednak utworzyć pełną kopię zapasową całego serwera. Kopię zapasową serwera można utworzyć podczas konserwacji lub tworzenia kopii zapasowej, po instalacji lub aktualizacji oprogramowania, przed przeniesieniem itd. W podanym przykładzie nie ma potrzeby regularnego tworzenia kopii zapasowej całych serwerów. Stare kopie zapasowe można usunąć ręcznie, ponieważ nie ma ich zbyt wiele.

1. Utwórz zasady tworzenia kopii zapasowych **[Wszystkie woluminy]** w skarbcu zarządzanym w węźle magazynowania. Wybierz opcje **Utwórz kopię zapasową później**, start ręczny oraz typ **Pełna** kopia zapasowa.

2. Utwórz grupę statyczną o nazwie S_1. Dodaj do niej wszystkie serwery. (Węzeł magazynowania można dodać, gdy skarbiec zarządzany nie znajduje się na lokalnych dyskach węzła. W przeciwnym razie kopia zapasowa magazynu archiwum zostanie umieszczona w nim samym).
3. Zastosuj zasady w grupie S_1. Upewnij się, że zasady zostały pomyślnie wdrożone na wszystkich serwerach. Stan wdrożenia zasad powinien zmienić się z **wdrażanie** na **wdrożone**, a status zasad na **OK**. Aby wyświetlić wynikowe plany tworzenia kopii zapasowych na każdym z serwerów:
   a. Przejdź do grupy **Wszystkie komputery** lub grupy S_1.
   b. Wybierz serwer.
   c. Wybierz kartę **Plany i zadania tworzenia kopii zapasowych** na panelu **Informacje**.

W razie potrzeby i przy nadarzającej się okazji do utworzenia kopii zapasowej jednego z serwerów przejdź do planu tworzenia kopii zapasowych, jak to opisano powyżej, wybierz plan i uruchom go.

Ochrona stacji roboczych

Oto sposób konfiguracji najpopularniejszego harmonogramu: cotygodniowa pełna kopia zapasowa i codzienna kopia zapasowa domyślnych folderów z dokumentami użytkowników. Ponadto będą przechowywane wyłącznie kopie zapasowe z ostatnich 7 dni.

1. Utwórz zasady tworzenie kopii zapasowych **[Folder wszystkich profilów]** w skarbcu zarządzanym w węźle magazynowania. Spowoduje to utworzenie kopii zapasowej folderu, w którym znajdują się profile użytkowników (na przykład C:\Documents and Settings w systemie Windows XP). Wybierz **Niestandardowy** schemat tworzenia kopii zapasowych.
   a. Zaplanuj pełną kopię zapasową w następujący sposób: **Co tydzień**, co tydzień w niedzielę, wykonaj zadanie jeden raz o godzinie 12:00:00. Ustawienia zaawansowane: funkcja Wake-on-LAN: włączona. Być może trzeba będzie rozłożyć uruchomienie w przedziale czasu, aby zoptymalizować wykorzystanie sieci i obciążenie procesora w węźle magazynowania.
   b. Zaplanuj przyrostową kopię zapasową w następujący sposób: **Co tydzień**, co tydzień w dnie robocze, wykonaj zadanie jeden raz o godzinie 20:00:00. Skonfiguruje również wymagane ustawienia zaawansowane.
   c. Skonfiguruj reguły przechowywania w następujący sposób: **Usuwaj kopie zapasowe starsze niż**: 7 dni. **W przypadku usuwania kopii zapasowej zawierającej zależności:** Konsoliduj kopie zapasowe. Dla innych reguł przechowywania pozostaw ustawienia domyślne. W oknie **Zastosuj reguły przechowywania** ustaw opcję **Po utworzeniu kopii zapasowej**.
2. Utwórz grupę dynamiczną o nazwie W_1. Jako kryteria określ: **%Windows%XP%** i **%Windows%Vista%**. W ten sposób każda stacja robocza zarejestrowana później na serwerze zarządzania zostanie dodana do tej grupy i objęta ochroną według tych samych zasad.
3. Zastosuj zasady w grupie W_1. Upewnij się, że zasady zostały pomyślnie wdrożone na wszystkich stacjach roboczych. Stan wdrożenia zasad powinien zmienić się z **wdrażanie** na **wdrożone**, a status zasad na **OK**. Aby wyświetlić wynikowe plany tworzenia kopii zapasowych na każdej stacji roboczej:
   a. przejdź do grupy **Wszystkie komputery** lub grupy W_1
   b. wybierz stację roboczą
   c. wybierz kartę **Plany i zadania tworzenia kopii zapasowych** na panelu **Informacje**.

   Zadania wynikowe utworzone na stacjach roboczych można również wyświetlić w widoku **Zadania**.
4. Do śledzenia codziennych czynności związanych z zasadami służy **Pulpit nawigacyjny** i widok **Zadania**. Po ustaleniu, czy wszystkie zadania zostały uruchomione zgodnie z planem, status zasad można sprawdzić tylko w widoku **Zasady tworzenia kopii zapasowych**.

Do codziennej ochrony danych można również użyć schematów tworzenia kopii zapasowych dziadek-ojciec-syn i Wieża Hanoi.

Ochrona maszyn wirtualnych

Komponent Acronis Backup & Recovery 10 Agent dla ESX/ESXi umożliwia elastyczną ochronę maszyn wirtualnych na wiele sposobów:

- Podłącz konsolę do urządzenia wirtualnego (Agent dla ESX/ESXi) i zdefiniuj plan tworzenia kopii zapasowych, który spowoduje tworzenie kopii zapasowych wszystkich lub niektórych maszyn wirtualnych.
- Podłącz konsolę do urządzenia wirtualnego (Agent dla ESX/ESXi) i zdefiniuj odrębny plan tworzenia kopii zapasowych dla każdej maszyny. Plan spowoduje tworzenie kopii zapasowych określonych woluminów.
- Zarejestruj urządzenie wirtualne (Agent dla ESX/ESXi) na serwerze zarządzania. Wszystkie maszyny wirtualne z wyjątkiem urządzenia wirtualnego pojawią się w grupie **Wszystkie maszyny wirtualne**. Maszyny te można zgrupować i zastosować do nich dowolne zasady tworzenia kopii zapasowych dysków lub woluminów.
- Zainstaluj na każdej maszynie wirtualnej agenta dla systemu Windows lub agenta dla systemu Linux. Zarejestruj maszyny na serwerze zarządzania. Maszyny będą traktowane jak komputery fizyczne. Do takich maszyn można zastosować zasady tworzenia kopii zapasowych. Można również zdefiniować plan tworzenia kopii zapasowych na każdej maszynie osobno. Jeśli dowolna z maszyn spełnia kryteria przynależności ustalone dla dynamicznej grupy komputerów fizycznych, zostanie objęta ochroną według zasad zastosowanych do tej grupy.

Zaawansowane wersje programu inne niż Virtual Edition (Acronis Backup & Recovery 10 Advanced Server, Advanced Server SBS Edition i Advanced Workstation) umożliwiają korzystanie tylko z ostatniej z powyższych metod.

2.15.3 Grupowanie zarejestrowanych komputerów

Natychmiast po zarejestrowaniu (s. 427) komputera na serwerze zarządzania, komputer pojawia się we wbudowanej grupie (s. 423) **Wszystkie komputery**. Zastosowanie zasad tworzenia kopii zapasowych zapewnia ochronę wszystkich zarejestrowanych komputerów. Problem polega na tym, że pojedyncze zasady mogą być niewystarczające ze względu na różne role komputerów.Archiwizowane dane są specyficzne dla każdego działu. Kopie zapasowe niektórych danych trzeba tworzyć bardzo często, a innych dwa razy do roku. Można więc utworzyć różne zasady stosowane do poszczególnych zestawów komputerów. W takim przypadku należy rozważyć utworzenie grup niestandardowych.

Grupy statyczne i dynamiczne

Można określić wprost komputery należące do grupy niestandardowej. Na przykład można wybrać wszystkie komputery księgowych. Po zastosowaniu zasad działu księgowości w tej grupie komputery księgowych zostaną objęte ochroną. Po zatrudnieniu nowego księgowego należy ręcznie dodać nowy komputer do grupy. Są to grupy statyczne (s. 423), ponieważ ich zawartość nigdy nie zmieni się, chyba że administrator ręcznie doda lub usunie komputer.

Jeśli dział księgowości stanowi oddzielną jednostkę organizacyjną usługi Active Directory, operacja ręczna nie jest wymagana. Jednostka organizacyjna księgowości jest określona jako kryterium przynależności do grupy. Po zatrudnieniu nowego księgowego nowy komputer zostanie dodany do grupy tuż po dodaniu go do jednostki organizacyjnej, a następnie automatycznie objęty ochroną. Są to grupy dynamiczne (s. 422), ponieważ ich zawartość zmienia się automatycznie.

Kryteria grupowania dynamicznego

Serwer Acronis Backup & Recovery 10 Management Server oferuje następujące kryteria przynależności do grup dynamicznych:

- system operacyjny (OS);
- jednostka organizacyjna Active Directory (OU);
- zakres adresów IP.

Można określić kilka kryteriów dla grup dynamicznych. Na przykład zestaw kryteriów „OS to Windows 2000, OS to Windows 2003, OU to Księgowość" jest interpretowany jako „wszystkie komputery z systemem Windows 2000 lub Windows 2003 należące do jednostki organizacyjnej Księgowość".

Grupę **Wszystkie komputery** można traktować jako grupę dynamiczną z jednym wbudowanym kryterium: dołącz wszystkie zarejestrowane komputery.

Korzystanie z grup niestandardowych

Grupowanie umożliwia organizowanie ochrony danych według działów firmy, domen Active Directory lub jednostek administracyjnych w ramach domeny, różnych populacji użytkowników, lokalizacji miejsc itp. Aby najlepiej wykorzystać kryterium jednostki organizacyjnej usługi Active Directory, warto odtworzyć hierarchię usługi Active Directory na serwerze zarządzania. Grupując według zakresu adresów IP, można uwzględnić topologię sieci.

Tworzone grupy można zagnieżdżać. Serwer zarządzania umożliwia obsługę maksymalnie 500 grup. Komputer może być członkiem jednej lub większej liczby grup.

Oprócz komputerów fizycznych można grupować maszyny wirtualne (s. 354) obsługiwane na zarejestrowanych serwerach wirtualizacji. Maszyny wirtualne mają własne kryteria grupy w zależności od właściwości.

Przykład

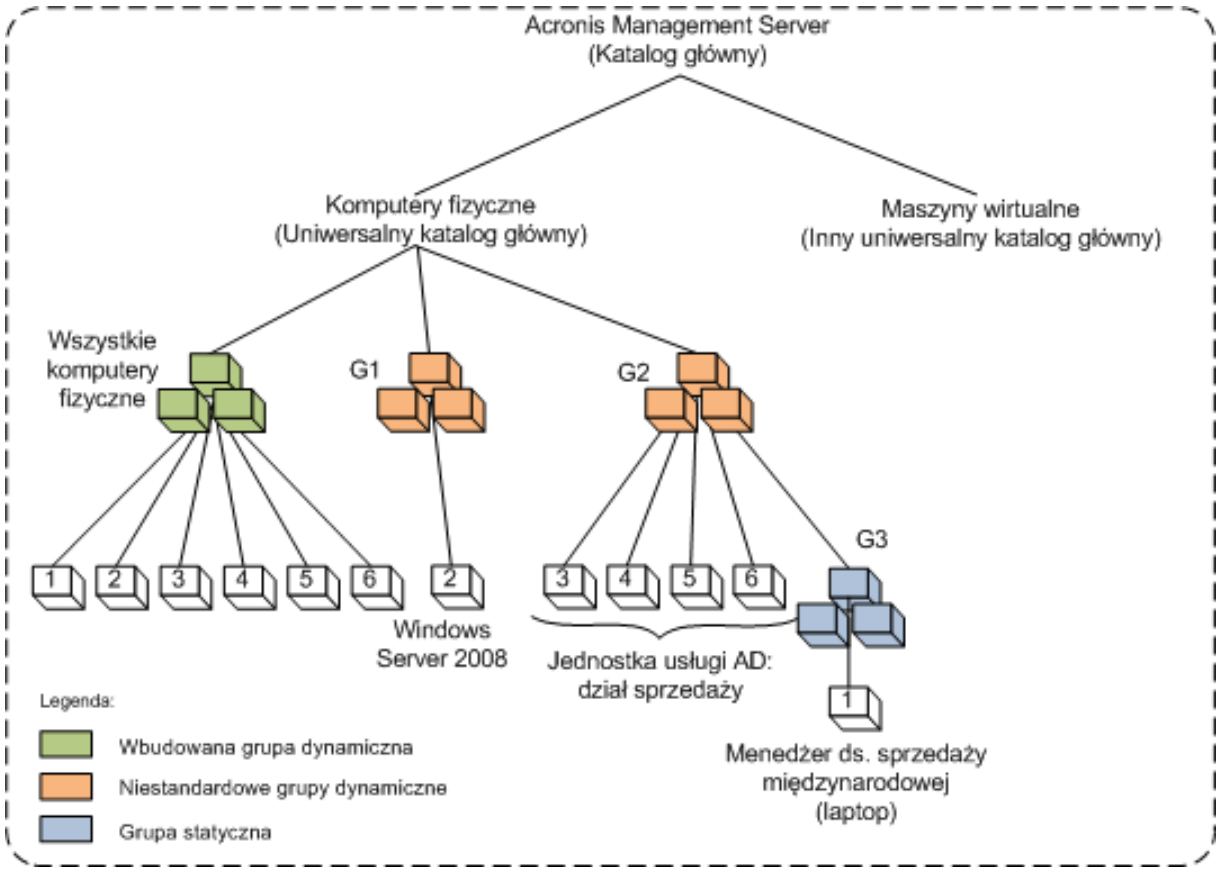
Poniższy schemat przedstawia przykład hierarchii grupy.

Na serwerze zarządzania jest zarejestrowanych sześć komputerów:

1 — laptop menedżera ds. sprzedaży międzynarodowej (Windows Vista);

2 — serwer, na którym znajduje się firmowa baza danych i udostępniony magazyn dokumentów (Windows Server 2008);

3, 4, 5, 6 — komputery sprzedawców (Windows XP) z „Działu sprzedaży” w jednostce organizacyjnej AD.



Przykład hierarchii grupy

Zasada tworzenia kopii zapasowych na serwerze musi być inna niż na stacjach roboczych. Administrator utworzył dynamiczną grupę G1, do której należą komputery z serwerowymi systemami operacyjnymi i zastosował do tej grupy zasadę tworzenia kopii zapasowych. Dowolny serwer dodawany do sieci i zarejestrowany na serwerze zarządzania będzie dodany do tej grupy i zasada zostanie na nim automatycznie zastosowana.

Aby chronić stacje robocze sprzedawców przy użyciu innej zasady, administrator utworzył grupę dynamiczną G2 używającą kryterium AD OU. Każda zmiana przynależności do OU zostanie uwzględniona w grupie G2. Odpowiednia zasada zostanie zastosowana do nowych komputerów w grupie OU i wycofana z komputerów wycofanych z OU.

Laptop menedżera ds. sprzedaży międzynarodowej nie należy do grupy OU, ale zawiera niektóre informacje zawarte na komputerach sprzedaży. Aby utworzyć kopię zapasową tych danych, administrator musi dodać „na siłę” ten laptop do grupy G2. Może to zrobić, tworząc grupę statyczną (G3) i przenosząc ją do grupy dynamicznej. Zasada zastosowana do grupy nadrzędnej (G2) będzie również zastosowana do grupy podrzędnej (G3), ale komputery należące do grupy G3 nie będą uważane za członków grupy G2, dlatego jej dynamiczny charakter nie zmieni się.

W rzeczywistości administrator najprawdopodobniej będzie wolał chronić komputer menedżera, stosując zasadę bezpośrednio do niego, bez dodawania go do żadnej grupy, zatem ten przypadek jest tylko przykładem zagnieżdżania różnych typów grup. Gdy do każdej grupy należy kilka komputerów, zagnieżdżanie jest przydatnym rozwiązaniem.

Operacje na grupach niestandardowych

Puste grupy (komputerów fizycznych lub maszyn wirtualnych) można utworzyć w uniwersalnym katalogu głównym lub w istniejących grupach i wypełnić je, ręcznie dodając komputery (grupy statyczne) lub dodając kryteria przynależności do grupie dynamicznej. Ponadto można

- edytować grupę, czyli wykonać następujące czynności:
  - zmiana nazwy grupy;
  - zmiana opisu grupy;
  - zmiana dynamicznych kryteriów przynależności;
- przekształcenie grupy statycznej w dynamiczną przez dodanie kryterium przynależności;
- przekształcenie grupy dynamicznej w statyczną za pomocą dwóch opcji:
  - zachowanie członków grupy;
  - usunięcie członków grupy;
- przeniesienie grupy (dowolnego typu) z katalogu głównego do innej grupy (dowolnego typu);
- przeniesienie grupy z grupy nadrzędnej do katalogu głównego;
- przeniesienie grupy z jednej grupy nadrzędnej (dowolnego typu) do innej (dowolnego typu);
- usunięcie grupy polegające na bezwarunkowym odłączeniu jej członków na wszystkich komputerach.

Operacje na grupach, w których zostały zastosowane zasady tworzenia kopii zapasowych, spowodują zmianę zasad na komputerach członkowskich. Jeśli w danym momencie komputer jest niedostępny lub nieosiągalny, status czynności zostanie zmieniony na „oczekująca” i zostanie ona wykonana, gdy komputer będzie dostępny.

Aby uzyskać informacje o sposobie wykonywania operacji, zobacz sekcję Operacje na grupach (s. 348).

2.15.4 Zasady komputerów i grup

Zagadnienia tej sekcji umożliwiają poznanie zasad automatycznego wdrażania i odwoływania zasad wykonywanych przez serwer zarządzania w przypadku zasady lub kilku zasad stosowanych do komputerów i grup zagnieżdżonych komputerów w różnych kombinacjach: kiedy zasady są odwoływane z komputera i grup lub kiedy komputer lub grupa są przenoszone z jednej grupy do drugiej.

Operacje na grupach, do których stosowane są zasady tworzenia kopii zapasowych powodują zmianę zasad na komputerach będących członkami grupy. Przy każdej zmianie hierarchii — to znaczy podczas przenoszenia, usuwania, tworzenia grup lub dodawania komputerów do grup statycznych lub gdy komputery wchodzą do grupy w oparciu o kryteria dynamiczne — może nastąpić bardzo wiele zmian dziedziczenia. Należy zapoznać się z tą sekcją, aby podejmowane czynności przynosiły pożądany rezultat oraz aby zrozumieć zautomatyzowane operacje serwera zarządzania Acronis Backup & Recovery 10 Management Server.

Co to znaczy stosować, wdrażać i odwoływać?

Stosowanie zasady ustanawia korespondencję pomiędzy zasadą a jednym lub wieloma komputerami. Proces ten ma miejsce wewnątrz bazy danych serwera zarządzania i nie zabiera wiele czasu.

Wdrażanie zasady przenosi ustanowioną korespondencję na komputery. W sensie fizycznym na każdym komputerze tworzona jest grupa zasad według konfiguracji ustanowionej w zasadzie.

Odwołanie zasady to czynność odwrotna w stosunku do stosowania i wdrażania łącznie. Odwołanie powoduje usunięcie korespondencji pomiędzy zasadą i jednym lub więcej komputerami, a następnie usunięcie zadania z komputera.

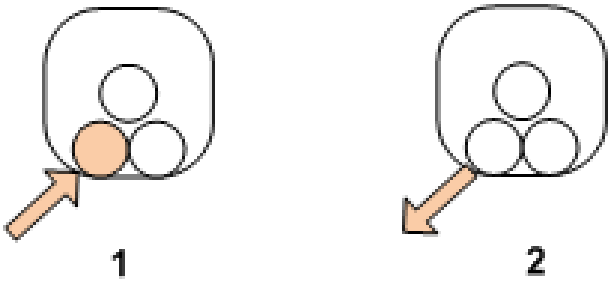
Jeśli w danym momencie komputer jest niedostępny lub nieosiągalny, zmiana w komputerze nastąpi kiedy będzie on dostępny. Oznacza to, że wdrożenie zasad na wielu komputerach nie jest czynnością natychmiastową. To samo dotyczy odwołania. Te dwa procesy mogą trwać i dlatego serwer zarządzania śledzi i wyświetla indywidualne statusy każdego komputera, z którym współpracuje, jak również status łączny zasad.

Stosowanie zasad do komputerów lub grup

Na poniższych diagramach kolejno ponumerowane schematy ilustrują efekt czynności o podanym numerze.

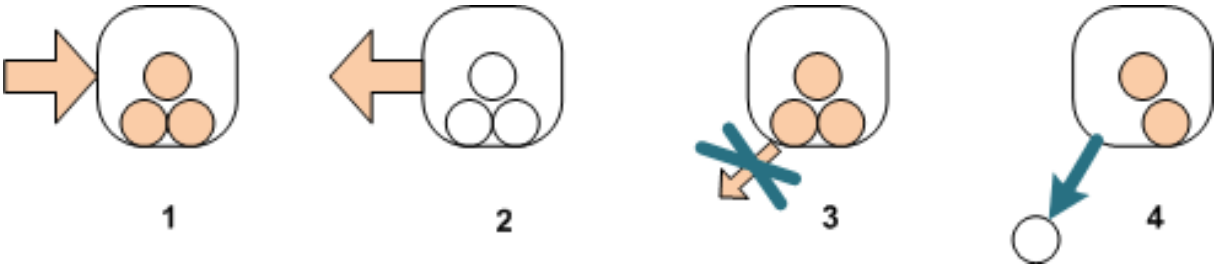
Kontener oznacza grupę, kolorowe kółko oznacza komputer, do którego zastosowano zasadę, ciemne kółko oznacza komputer, do którego dwukrotnie zastosowano tę samą zasadę, białe kółko oznacza komputer, do którego nie zastosowano żadnej zasady.

Zasada na komputerze



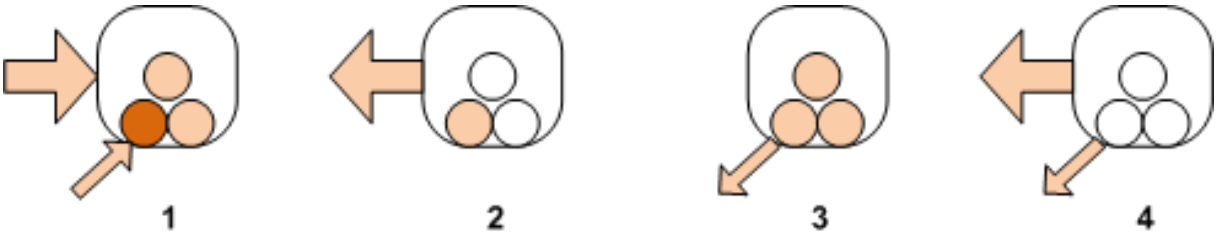
1. Zasadę można zastosować do komputera.
2. Zasadę można odwołać z komputera.

Zasada w grupie



1. Zasadę można zastosować do grupy.
2. Zasadę można odwołać z grupy.
3. Nie można odwołać z komputera zasady zastosowanej do grupy.
4. Aby odwołać zasadę z komputera, należy usunąć komputer z grupy.

Ta sama zasada zastosowana do grupy i do komputera



1. Tę samą zasadę można zastosować do grupy i do komputera. Po kolejnym zastosowaniu tej samej zasady na komputerze nic się nie zmienia, ale serwer pamięta, że zasadę zastosowano dwukrotnie.
2. Po odwołaniu zasady z grupy pozostaje ona na komputerze.
3. Po odwołaniu zasady z komputera pozostaje ona w grupie, a zatem również na komputerze.
4. Aby całkowicie odwołać zasadę z komputera, należy odwołać ją zarówno z grupy, jak i z komputera.

Operacje na komputerze

Ta sekcja pokazuje w uproszczony sposób, co się dzieje z zasadami na komputerze przenoszonym, kopiowanym lub usuwanym z grupy.

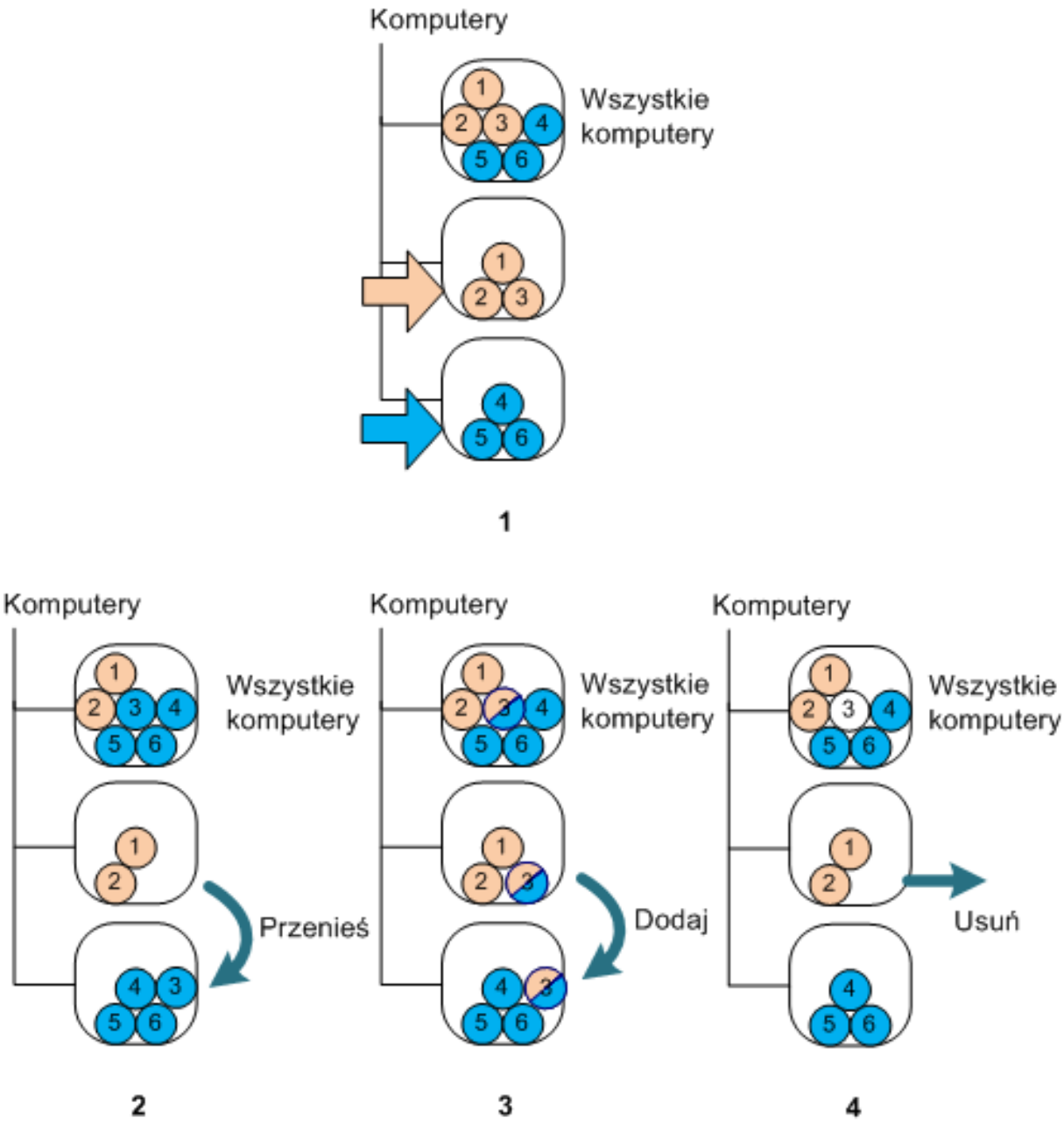
Na wykresie poniżej pojemnik zawierający koła oznacza grupę, natomiast koło w jednym kolorze oznacza komputer z jedną stosowaną zasadą, koło z dwoma kolorami oznacza komputer z dwoma stosowanymi zasadami, a białe koło oznacza komputer bez żadnych stosowanych zasad.

1. Stan początkowy: dwie grupy niestandardowe zawierają różne komputery. Do jednej z grup zastosowana jest zasada, a do innej grupy inna zasada. Następne schematy pokazują rezultaty określonych czynności.

2. **Przenieś do innej grupy:** Komputer nr 3 został przeniesiony z jednej grupy do drugiej. Zasada „pomarańczowa” została odwołana, a zasada „niebieska” zastosowana do komputera.

3. **Dodaj do innej grupy**: Komputer nr 3 został dodany do innej grupy. Stał się członkiem obu grup. Zasada „niebieska” została zastosowana, ale zasada „pomarańczowa” pozostała na komputerze.

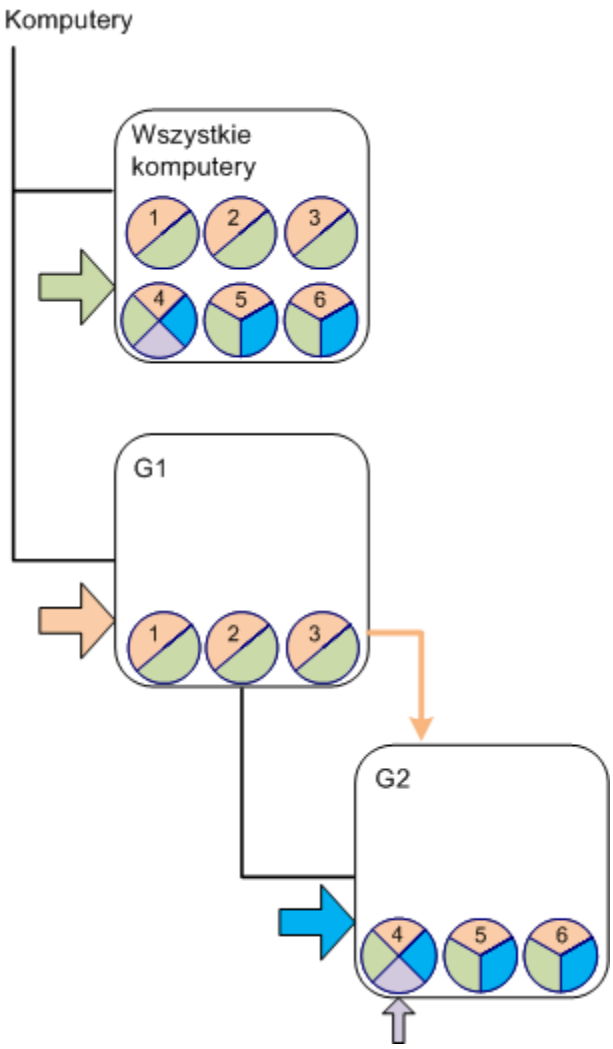
4. **Usuń z grupy**: Komputer nr 3 został usunięty z grupy. Zasada „pomarańczowa” została odwołana z komputera. Komputer pozostał w grupie **Wszystkie komputery**.



Dziedziczenie zasad

Dziedziczenie zasad można łatwo zrozumieć przy założeniu, że komputer może należeć tylko do jednej grupy poza grupą **Wszystkie komputery**. Rozpocznijmy od tego uproszczonego podejścia.

Na poniższym schemacie kontener oznacza grupę, dwukolorowe kółko oznacza komputer z dwoma zastosowanymi zasadami, trójkolorowe kółko oznacza komputer z trzema zastosowanymi zasadami itd.



Oprócz grupy **Wszystkie komputery** istnieje grupa główna G1 i grupa G2, będąca jej grupą podrzędną.

„Zielona” zasada zastosowana do grupy **Wszystkie komputery** jest dziedziczona przez wszystkie komputery.

„Pomarańczowa” zasada zastosowana do grupy G1 jest dziedziczona przez komputery należące do grupy G1 i wszystkie grupy, zarówno bezpośrednio jak i pośrednio podrzędne.

„Niebieska” zasada zastosowana do grupy G2 jest dziedziczona tylko przez komputery należące do tej grupy, ponieważ grupa G2 nie ma grup podrzędnych.

„Fioletowa” zasada jest zastosowana bezpośrednio do komputera 4. Będzie znajdowała się na komputerze 4 niezależnie od jego przynależności do jakiejkolwiek grupy.

Przyjmijmy, że utworzono grupę G3 jako grupę główną. Jeśli nie zastosujemy do niej żadnych zasad, wszystkie należące do niej komputery będą miały kolor „zielony”. Ale jeśli dodamy do grupy G3 np. komputer 1, będzie on miał zarówno kolor „pomarańczowy”, jak i „zielony”, pomimo, że grupa G3 nie ma nic wspólnego z „pomarańczową” zasadą.

Dlatego śledzenie dziedziczenia zasad od samego początku hierarchii jest tak trudne, gdy komputer należy do wielu grup.

W rzeczywistości o wiele łatwiej jest sprawdzać dziedziczenie od strony komputera. Aby to zrobić, należy przejść do dowolnej grupy, do której należy komputer, wybrać go, a następnie wybrać kartę **Zasady tworzenia kopii zapasowych** na panelu **Informacje**. W kolumnie **Dziedziczenie** widać, czy zasada jest dziedziczona, czy zastosowana bezpośrednio do komputera. Aby wyświetlić kolejność dziedziczenia zasady, należy kliknąć **Eksploruj dziedziczenie**. W naszym przykładzie nazwy zasad w kolumnie **Dziedziczenie** i kolejność dziedziczenia będą następujące:

Komputer	**Nazwa zasady**	**Dziedziczenie**	**Kolejność dziedziczenia**
1 lub 2 lub 3	„zielona”	Dziedziczona	Wszystkie komputery -> 1 lub 2 lub 3
	„pomarańczowa”	Dziedziczona	G1 -> 1 lub 2 lub 3
4	„zielona”	Dziedziczona	Wszystkie komputery -> 4
	„pomarańczowa”	Dziedziczona	G1 -> G2 -> 4
	„niebieska”	Dziedziczona	G2 -> 4
	„fioletowa”	Zastosowane bezpośrednio	

5 lub 6	„zielona”	Dziedziczona	Wszystkie komputery -> 5 lub 6
	„pomarańczowa”	Dziedziczona	G1 -> G2 -> 5 lub 6
	„niebieska”	Dziedziczona	G2 -> 5 lub 6

2.15.5 Stany i statusy zasad tworzenia kopii zapasowych

Zarządzanie scentralizowane zakłada, że administrator może monitorować stan całej infrastruktury produktu przy użyciu kilku zrozumiałych parametrów. Parametry te obejmują stan i status zasad tworzenia kopii zapasowych. Problemy, jeśli występują, są przekazywane z samego dołu infrastruktury (zadania na komputerach zarządzanych) do skumulowanego statusu zasad. Administrator może natychmiast sprawdzić status. Jeśli nie jest on prawidłowy, można przejść do szczegółów problemu, wykonując kilka kliknięć.

Ta sekcja pomaga zrozumieć stany i statusy zasad, jakie są wyświetlane przez serwer zarządzania.

Stan wdrażania zasad na komputerze

Aby sprawdzić ten parametr, wybierz dowolną grupę zawierającą komputer w drzewie, a następnie wybierz komputer oraz kartę **Zasady tworzenia kopii zapasowych** w panelu **Informacje**.

Po zastosowaniu zasad do komputera lub grupy komputerów serwer wdraża zasady na komputerach. Agent tworzy plan tworzenia kopii zapasowych na każdym komputerze. Podczas przenoszenia zasad na komputer i tworzenia planu kopii zapasowych stan wdrażania zasad na komputerze to **Wdrażanie**.

Po pomyślnym utworzeniu planu tworzenia kopii zapasowych stan zasad na komputerze zmienia się na **Wdrożone**.

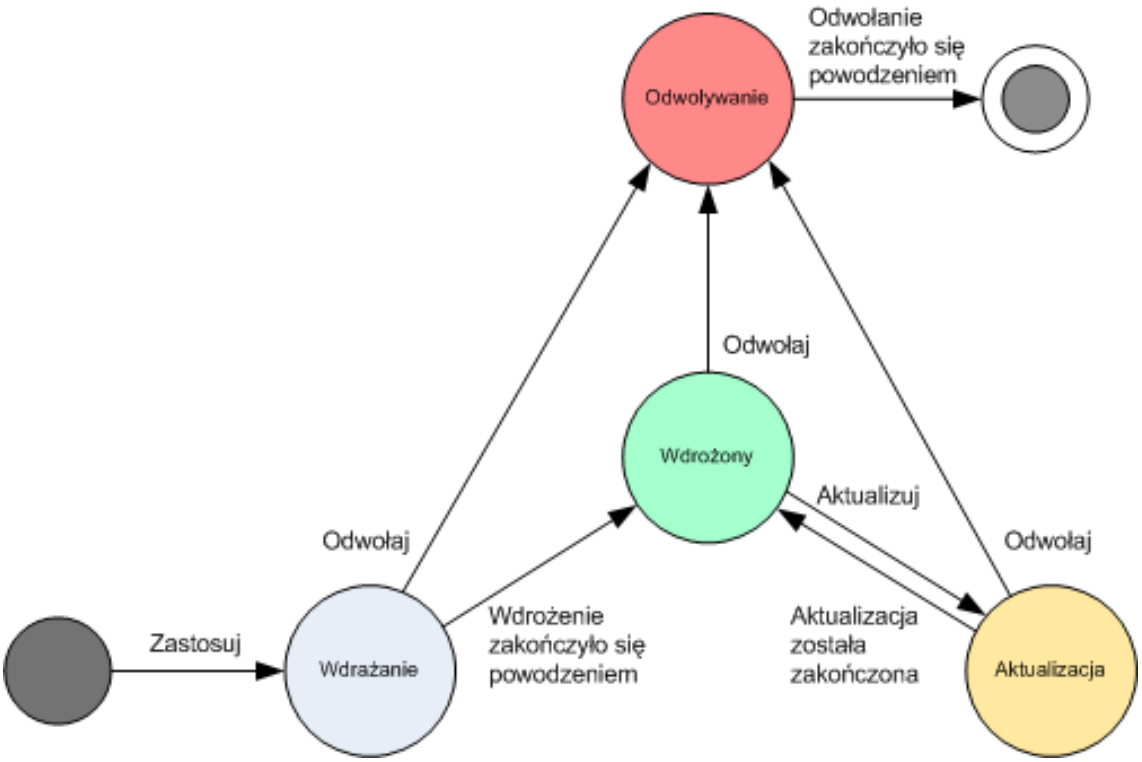
Może pojawić się konieczność modyfikacji zasad z jakiegoś powodu. Po zatwierdzeniu zmian serwer zarządzania aktualizuje zasady na wszystkich komputerach, na których zostały one wdrożone. Podczas przenoszenia zmian na komputer i aktualizacji planu tworzenia kopii zapasowych przez agenta stan zasad na komputerze to **Aktualizacja**. Po wykonaniu aktualizacji stan zasad zmienia się ponownie na **Wdrożone**. Stan ten oznacza, że zasady działają i nie są zmieniane w danym momencie.

Zasady zmienione w trakcie wdrażania pozostają w stanie **Wdrażanie**. Serwer zarządzania rozpoczyna wdrażanie zmodyfikowanych zasad od początku.

Może pojawić się konieczność odwołania zasad z komputera lub z grupy, do której komputer należy. Po zatwierdzeniu zamian serwer zarządzania odwołuje zasady z komputera. Podczas przenoszenia zmian na komputer i usuwania planu tworzenia kopii zapasowych z komputera przez agenta stan zasad na komputerze to **Odwoływanie**.

Można zmienić warunki grupowania lub mogą zmienić się właściwości komputera, tak że komputer opuszcza jedną grupę i dołącza do innej. Może to spowodować odwołanie jednej z zasad i wdrożenie innej. W tym przypadku stan pierwszej zasady na komputerze to **Odwoływanie**, a stan drugiej zasady to **Wdrażanie**. Zasady mogą pojawić się w graficznym interfejsie użytkownika jednocześnie lub jedna po drugiej.

Wykres stanu zasad tworzenia kopii zapasowych



Status zasad na komputerze

Aby sprawdzić ten parametr, wybierz dowolną grupę zawierającą komputery w drzewie, a następnie wybierz komputer oraz kartę **Zasady tworzenia kopii zapasowych** w panelu **Informacje**.

W każdym stanie wdrażania zasada tworzenia kopii zapasowych może posiadać jeden z następujących statusów: **Błąd**, **Ostrzeżenie** lub **OK**. Gdy zasada jest w stanie **Wdrożone**, jej status pokazuje, na ile pomyślnie jest wykonywana. Gdy zasada znajduje się w innym stanie, jej status pokazuje, na ile pomyślnie przebiega proces zmiany.

Status zasady, gdy na komputerze nie można znaleźć danych przeznaczonych do kopii zapasowej

Zasadę tworzenia kopii zapasowych można zastosować do komputera, na którym nie ma danych spełniających reguły wyboru (p. 426). Podczas wdrażania zasady nie są rejestrowane błędy ani ostrzeżenia, ponieważ przyjmuje się, że dane mogą się pojawić w przyszłości. Plan tworzenia kopii zapasowych jest tworzony w normalny sposób i stan zasad zmienia się na **Wdrożone**.

Jeśli po rozpoczęciu wykonywania zadania program nie znajdzie danych do utworzenia kopii zapasowej, zadanie zakończy się niepowodzeniem, a stan zasad zmieni się na **Błąd**. Jeśli program znajdzie co najmniej jeden z elementów danych, zadanie zakończy się powodzeniem z ostrzeżeniem. Stan zasad zmieni się w odpowiedni sposób.

Wykonywanie zadań tworzenia kopii zapasowych rozpoczyna się zgodnie z harmonogramem określonym przez zasady i daje podobny wynik, dopóki wszystkie elementy danych nie pojawią się na komputerze lub zasady zostaną edytowane w celu wykluczenia nieistniejących elementów.

Przykłady

Przyjmijmy, że reguła wyboru określa, że zasady mają obejmować utworzenie kopii zapasowych woluminów D: i F:. Zasady są stosowane na komputerach z systemem Linux oraz Windows. Po rozpoczęciu tworzenia pierwszej kopii zapasowej, zasady otrzymują status **Błąd** na komputerach z

systemem Linux oraz na tych komputerach z systemem Windows, na których nie ma takich woluminów. Zasada mają status **Ostrzeżenie** na komputerach, na których znajduje się wolumin D: lub F:, chyba że wystąpi zdarzenie powodujące powstanie błędu.

Zasady, która mają utworzyć kopie zapasowe woluminów [System] i /dev/sda1 będą miały status **Ostrzeżenie** na komputerach z systemem Windows (ponieważ wolumin /dev/sda nie zostanie znaleziony) oraz na komputerach z systemem Linux, na których istnieje wolumin /dev/sda1 (ponieważ wolumin [System] nie zostanie znaleziony). Zasady będą miały status **Błąd** na komputerach z systemem Linux, na których nie ma urządzenia SCSI.

Poniższa tabela zawiera szczegółowe informacje.

Stan	Status	Opis
Wdraża-nie	**Błąd**	Dziennik wdrażania zawiera błędy, na przykład kończy się miejsce na dysku.
	Ostrzeże-nie	Dziennik wdrażania zawiera ostrzeżenia: komputer przeszedł w tryb offline w trakcie wdrażania lub nie można nawiązać połączenia przez N dni.
	OK	Dziennik wdrażania nie zawiera błędów ani ostrzeżeń.
Wdrożone	**Błąd**	Status odpowiedniego planu tworzenia kopii zapasowych to **Błąd.**
	Ostrzeże-nie	Status odpowiedniego planu tworzenia kopii zapasowych to **Ostrzeżenie.**
	OK	Status odpowiedniego planu tworzenia kopii zapasowych to **OK.**
Aktuali-zacja	**Błąd**	Dziennik aktualizacji zawiera błędy: nie można usunąć zablokowanego zadania, wykonywanie usługi Acronis zostało zatrzymane.
	Ostrzeże-nie	Dziennik aktualizacji zawiera ostrzeżenia.
	OK	Dziennik aktualizacji nie zawiera błędów ani ostrzeżeń.
Odwoły-wanie	**Błąd**	Dziennik odwołań zawiera błędy.
	Ostrzeże-nie	Dziennik odwołań zawiera ostrzeżenia.
	OK	Dziennik odwołań nie zawiera błędów ani ostrzeżeń.

Oprócz stanu i statusu wdrażania zasad związanych z określonym komputerem istnieją stan i status zasad tworzenia kopii zapasowych grupy komputerów oraz łączny stan i status wdrożenia zasad.

Stan wdrażania zasad w grupie

Aby sprawdzić ten parametr, wybierz **Komputery** w drzewie, a następnie wybierz grupę i kartę **Zasady tworzenia kopii zapasowych** w panelu **Informacje**.

Ten stan określa się jako połączenie stanów wdrożenia zasad na komputerach znajdujących się w grupie i jej grupach podrzędnych.

Na przykład, zasada została zastosowana do grupy składającej się z komputerów A i B. W trakcie wdrażania zasad na obu komputerach stan zasad grupy będzie miał wartość „Wdrażanie”. Jeśli wdrożenie zakończy się na jednym z komputerów, podczas gdy będzie kontynuowane na drugim, stan będzie miał wartość „Wdrażanie, Wdrożone”. Kiedy wdrażanie zakończy się na obu komputerach, stan będzie miał wartość „Wdrożone”.

Status zasad w grupie

Aby sprawdzić ten parametr, wybierz **Komputery** w drzewie, a następnie wybierz grupę i kartę **Zasady tworzenia kopii zapasowych** w panelu **Informacje**.

Ten status określa się jako najbardziej poważny status zasad na komputerach zawartych w grupie i jej grupach podrzędnych. Jeśli zasada nie jest w danym momencie stosowana do żadnego z komputerów, jej status będzie miał wartość „OK”.

Skumulowany stan i status zasady

Oprócz statusu i stanu wdrażania w odniesieniu do konkretnego komputera lub grupy, zasada tworzenia kopii zapasowych ma skumulowany stan wdrażania i skumulowany status.

Skumulowany stan zasady tworzenia kopii zapasowych

Aby wyświetlić ten parametr, wybierz w drzewie **Zasady tworzenia kopii zapasowych**. W kolumnie **Stan wdrażania** wyświetlony jest skumulowany stan wdrażania dla każdej zasady.

Ten stan jest określony jako kombinacja stanów wdrażania zasady na wszystkich komputerach, na których została zastosowana (bezpośrednio lub w wyniku dziedziczenia). Jeśli zasada nie jest aktualnie zastosowana na żadnym komputerze, nie ma ona stanu wdrożenia i w kolumnie znajduje się informacja „Niezastosowane”.

Na przykład: zasadę zastosowano na komputerze A. Zasada została pomyślnie wdrożona. Następnie użytkownik zmodyfikował zasadę i natychmiast zastosował ją do grupy składającej się z komputerów B i C. Trzeba zaktualizować zasadę na komputerze A i wdrożyć ją na komputerach B i C. W czasie trwania tego procesu skumulowany stan zasady może mieć wartość „Aktualizacja, Wdrażanie”, następnie zmienić się na „Aktualizacja, Wdrożone” lub „Wdrożone, Wdrażanie” i zwykle zakończy się jako „Wdrożone”.

Skumulowany status zasady tworzenia kopii zapasowych

Aby wyświetlić ten parametr, wybierz w drzewie **Zasady tworzenia kopii zapasowych**. W kolumnie **Status** wyświetlony jest skumulowany status wdrażania dla każdej zasady.

Status ten jest określony jako najistotniejszy status zasady na wszystkich komputerach, na których jest zastosowana. Jeśli zasada nie jest zastosowana na żadnym komputerze, jej status to „OK”.

2.15.6 Deduplikacja

W tej sekcji omówiono deduplikację, czyli mechanizm mający na celu eliminację powtarzających się danych przez zachowywanie w archiwach tylko jednego egzemplarza identycznych elementów.

Omówienie

Deduplikacja to proces minimalizowania miejsca do przechowywania danych poprzez wykrywanie powtarzających się danych i przechowywanie identycznych danych tylko raz.

Jeśli na przykład skarbiec zarządzany z aktywną usługą deduplikacji zawiera dwie kopie tego samego pliku — w tym samym lub różnych archiwach — plik taki będzie przechowywany tylko raz, a zamiast drugiego pliku w skarbcu znajdzie się tylko łącze do niego.

Deduplikacja umożliwia również zmniejszenie obciążenia sieci: jeśli podczas tworzenia kopii zapasowej, program wykryje plik lub blok dysku, będący duplikatem już przechowywanych danych, jego zawartość nie będzie przesyłana w sieci.

Deduplikację wykonuje się na blokach dysku (deduplikacja na poziomie bloków) i plikach (deduplikacja na poziomie plików) — odpowiednio dla kopii zapasowej na poziomie dysku i kopii zapasowej na poziomie pliku.

W programie Acronis Backup & Recovery 10 deduplikacja składa się z dwóch etapów:

Deduplikacja w miejscu źródłowym

Wykonywana na komputerze zarządzanym podczas tworzenia kopii zapasowej. Acronis Backup & Recovery 10 Agent korzysta z węzła magazynowania w celu określenia danych przeznaczonych do deduplikacji i nie przesyła danych, których duplikaty już istnieją w skarbcu.

Deduplikacja w miejscu docelowym

Wykonywana w skarbcu po zakończeniu tworzenia kopii zapasowej. Węzeł magazynowania analizuje archiwa skarbca i przeprowadza deduplikację danych w skarbcu.

Podczas tworzenia planu tworzenia kopii zapasowej istnieje możliwość wyłączenia funkcji deduplikacji w miejscu źródłowym dla danego planu. Może to prowadzić do szybszego tworzenia kopii zapasowych, ale za to do większego obciążenia sieci i węzła magazynowania.

Skarbiec deduplikacji

Skarbiec centralny zarządzany z włączoną funkcją deduplikacji określany jest mianem *skarbca deduplikacji*. Podczas tworzenia skarbca centralnego zarządzanego można aktywować lub dezaktywować funkcję deduplikacji. Skarbca deduplikacji nie można utworzyć na urządzeniu taśmowym.

Baza danych deduplikacji

Węzeł magazynowania Acronis Backup & Recovery 10 Storage Node zarządzający skarbcem deduplikacji utrzymuje bazę danych deduplikacji, która zawiera wartości skrótów wszystkich elementów przechowywanych w skarbcu z wyjątkiem tych, które nie mogą zostać poddane deduplikacji, na przykład plików zaszyfrowanych.

Baza deduplikacji jest przechowywana w folderze określonym w polu **Ścieżka bazy danych** w widoku **Utwórz skarbiec centralny** podczas tworzenia skarbca. Bazę deduplikacji można utworzyć tylko w folderze lokalnym.

Rozmiar bazy danych deduplikacji wynosi około jednego procenta całkowitego rozmiaru archiwów w skarbcu. Innymi słowy każdy terabajt nowych (nieduplikowanych) danych powoduje dodanie około 10 GB pojemności bazy danych.

Jeśli w przypadku uszkodzenia bazy danych lub utraty węzła magazynowania w skarbcu zachowane zostaną archiwa i folder zawierający metadane, nowy węzeł magazynowania przeszuka ponownie skarbiec i odtworzy bazę danych.

Zasada działania deduplikacji

Deduplikacja w źródle

Podczas tworzenia kopii zapasowej w skarbcu deduplikacji agent programu Acronis Backup & Recovery 10 odczytuje kopiowane elementy — bloki dysku w przypadku kopii zapasowej dysku lub pliki w przypadku kopii zapasowej plików — i oblicza wartość odcisku dla każdego z elementów. Taki odcisk, zwany często *wartością skrótu*, stanowi unikatową identyfikację zawartości elementu w skarbcu.

Przed przesłaniem elementu do skarbca agent wysyła kwerendę do bazy danych deduplikacji, aby ustalić, czy wartość skrótu elementu jest taka sama jak jednego z elementów już przechowywanych.

Jeśli tak, agent wysyła tylko wartość skrótu elementu. Jeśli nie, agent wysyła sam element.

Niektórych elementów, takich jak pliki zaszyfrowane lub bloki dysku o niestandardowym rozmiarze, nie można poddać deduplikacji i agent zawsze wysyła takie elementy do skarbca bez obliczania ich wartości skrótu. Więcej informacji na temat ograniczeń deduplikacji na poziomie plików i na poziomie bloków znajduje się w sekcji Ograniczenia deduplikacji (s. 85).

Deduplikacja w miejscu docelowym

Gdy zakończy się tworzenie kopii zapasowej w skarbcu deduplikacji, węzeł magazynowania uruchamia **zadanie indeksowania** w celu deduplikacji danych w skarbcu w następujący sposób:

1. Przenosi elementy (bloki dysku lub pliki) z archiwów do specjalnego pliku wewnątrz skarbca, umieszczając w nim duplikaty tylko raz. Plik ten nazywany jest **magazynem danych deduplikacji**. Jeśli w skarbcu znajdują się kopie zapasowe utworzone na poziomie dysków i na poziomie plików, program utworzy dla nich dwa oddzielne magazyny danych. Elementy, w przypadku których duplikacja jest niemożliwa, pozostają w archiwach.
2. W archiwach zastępuje on przeniesione elementy odpowiednimi odwołaniami do nich.

W efekcie skarbiec zawiera pewną liczbę unikatowych, zdeduplikowanych elementów, a do każdego z nich w archiwach skarbca znajduje się jedno lub więcej odwołań.

Wykonanie zadania indeksowania może potrwać trochę dłużej. Stan zadania jest widoczny w widoku **Zadania** na serwerze zarządzania.

Kompaktowanie

Gdy ze skarbca zostanie usunięta — ręcznie lub podczas czyszczenia — jedna lub więcej kopii zapasowych bądź archiwów, skarbiec może zawierać elementy, do których nie odwołuje się żadne archiwum. Elementy takie są usuwane przez **zadanie kompaktowania**, które jest zaplanowanym zadaniem wykonywanym w węźle magazynowania.

Domyślnie zadanie kompaktowania jest uruchamiane w każdą niedzielę w nocy o godzinie 3:00. Harmonogram zadania można zmienić w sposób opisany w sekcji Czynności dotyczące węzłów magazynowania (s. 363) w punkcie „Zmiana harmonogramu zadania kompaktowania”. Zadanie można również uruchomić lub zatrzymać w widoku **Zadania**.

Ponieważ usuwanie nieużywanych elementów wymaga użycia dużej ilości zasobów, zadanie kompaktowania usuwa elementy tylko po zgromadzeniu wystarczającej ilości danych do usunięcia. Próg jest określony przez parametr konfiguracyjny **Próg uruchomienia kompaktowania** (s. 379).

Najefektywniejsza deduplikacja

Poniżej wymieniono sytuacje, w których deduplikacja przynosi najlepszy efekt:

- Tworzenie kopii zapasowej podobnych danych z różnych źródeł w **trybie pełnej kopii zapasowej**. Sytuacja taka ma miejsce, gdy tworzona jest kopia zapasowa systemów operacyjnych i aplikacji wdrożonych w sieci z jednego źródła.
- Tworzenie **przyrostowych kopii zapasowych** podobnych danych z różnych źródeł, pod warunkiem, że **zmiany danych są również podobne**. Sytuacja taka ma miejsce, gdy wdrażane są aktualizacje systemów, a następnie tworzona jest przyrostowa kopia zapasowa.
- Tworzenie **przyrostowych kopii zapasowych** danych, które same się nie zmieniają, ale **zmienia się ich lokalizacja.** Sytuacja taka ma miejsce, gdy wiele fragmentów danych krąży w sieci lub w

jednym systemie. Każdy ruch fragmentu danych jest uwzględniany w przyrostowej kopii zapasowej, co powoduje, że kopia się rozrasta, a nie zawiera żadnych nowych danych. Deduplikacja ułatwia rozwiązanie tego problemu: za każdym razem, gdy określony element pojawi się w nowym miejscu, zapisywane jest odwołanie do tego elementu, a nie on sam.

Deduplikacja i przyrostowe kopie zapasowe

W przypadku losowych zmian danych deduplikacja przyrostowej kopii zapasowej nie przyniesie większych efektów, ponieważ:

- elementy zdeduplikowane, które nie uległy zmianie, nie są uwzględniane w przyrostowej kopii zapasowej;
- elementy zdeduplikowane, które uległy zmianie, nie są już identyczne i dlatego nie będą dłużej deduplikowane.

Sprawdzone praktyki dotyczące deduplikacji

W trakcie korzystania z deduplikacji postępuj zgodnie z następującymi zaleceniami:

- Podczas tworzenia skarbca deduplikacji **umieść skarbiec i bazę danych deduplikacji na oddzielnych dyskach.** Spowoduje to przyspieszenie deduplikacji, ponieważ wiąże się ona z jednoczesnym intensywnym używaniem skarbca i bazy danych.
- Indeksowanie kopii zapasowej wymaga, aby w skarbcu znajdowało się **wolne miejsce o minimalnej wielkości równej rozmiarowi archiwum, do którego należy kopia zapasowa, pomnożonemu przez 1,1**. Jeśli w skarbcu jest za mało wolnego miejsca, zadanie indeksowania zakończy się niepowodzeniem i rozpocznie ponownie po 5–10 minutach (przy założeniu, że część miejsca została zwolniona w wyniku czyszczenia lub przez inne zadanie indeksowania). Im więcej wolnego miejsca w skarbcu, tym szybciej rozmiar archiwów zostanie zredukowany do możliwego minimum.
- W przypadku tworzenia kopii zapasowej wielu systemów o podobnej zawartości **utwórz najpierw kopię jednego takiego systemu.** Dzięki temu węzeł magazynowania Acronis Backup & Recovery 10 Storage Node wykona indeksację wszystkich plików systemu jako potencjalnych elementów deduplikacji. Wskutek tego tworzenie kopii zapasowych będzie szybsze, a ruch sieciowy mniejszy (z powodu efektywnej deduplikacji w źródle), niezależnie od tego, czy kopie zapasowe będą tworzone równocześnie, czy nie.

  Przed przystąpieniem do tworzenia kolejnych kopii zapasowych upewnij się, że **zadanie indeksowania zakończyło** deduplikację pierwszej kopii zapasowej i jest aktualnie w stanie bezczynności. Stan zadania indeksowania można wyświetlić na liście zadań w serwerze Acronis Backup & Recovery 10 Management Server.

Współczynnik deduplikacji

Współczynnik deduplikacji to stosunek rozmiaru archiwów w skarbcu deduplikacji do rozmiaru, które miałyby te archiwa w skarbcu bez deduplikacji.

Załóżmy na przykład, że tworzona jest kopia zapasowa dwóch plików o identycznej zawartości z dwóch różnych komputerów. Jeśli rozmiar każdego z plików wynosi jeden gigabajt, rozmiar kopii zapasowych w skarbcu bez deduplikacji będzie wynosić około 2 GB. W skarbcu deduplikacji będzie to około 1 GB, a więc współczynnik deduplikacji wyniesie 2:1 lub 50%.

Jeśli natomiast oba pliki będą mieć różną zawartość, rozmiary kopii zapasowych w skarbcach deduplikacji oraz bez deduplikacji będą takie same (2 GB), a jej współczynnik wyniesie 1:1 lub 100%.

Jakiego współczynnika można się spodziewać

Mimo że w niektórych sytuacjach współczynnik deduplikacji może być bardzo wysoki (w poprzednim przykładzie przy większej liczbie komputerów wartość współczynnika mogłaby wzrosnąć do 3:1, 4:1 itd.), w typowym środowisku można oczekiwać współczynnika między 1,2:1 a 1,6:1.

W kolejnym przykładzie przyjmijmy bardziej realistyczne założenia. Na dwóch komputerach z podobnymi dyskami tworzone są kopie zapasowe na poziomie plików i na poziomie dysku. Na każdym komputerze pliki wspólne dla obu komputerów zajmują 50% miejsca na dysku (na przykład 1 GB), a pliki unikatowe — pozostałe 50% (kolejny 1 GB).

W tym przypadku w skarbcu deduplikacji rozmiar kopii zapasowej pierwszego komputera wyniesie 2 GB, a drugiego komputera — 1 GB. W skarbcu bez deduplikacji kopie zapasowe zajęłyby łącznie 4 GB. W efekcie współczynnik deduplikacji wyniesie 4:3, czyli około 1,33:1.

W przypadku trzech komputerów współczynnik wyniesie 1,5:1, a przy czterech komputerach — 1,6:1. W miarę dodawania kolejnych komputerów do kopii zapasowej w tym samym skarbcu wartość współczynnika będzie dążyć do 2:1. Oznacza to, że zamiast kupowania urządzenia pamięci masowej o pojemności 20 TB, wystarczy kupić urządzenie o pojemności 10 TB.

Rzeczywiste zmniejszenie ilości zajmowanego miejsca zależy od wielu czynników, takich jak typ danych w tworzonej kopii zapasowej, częstotliwość tworzenia kopii zapasowych oraz okres ich przechowywania.

Ograniczenia deduplikacji

Ograniczenia deduplikacji na poziomie bloków

Podczas tworzenia kopii zapasowej dysku w archiwum skarbca deduplikacji w poniższych przypadkach nie następuje deduplikacja bloków dysku woluminu:

- Jeśli wolumin jest woluminem skompresowanym
- Jeśli rozmiar jednostki alokacji woluminu — nazywany również rozmiarem klastra lub rozmiarem bloku — jest niepodzielny przez 4 KB

  Wskazówka: *Rozmiar jednostki alokacji na większości woluminów NTFS i ext3 wynosi 4 KB, zatem umożliwia deduplikację na poziomie bloków. Inne przykładowe rozmiary jednostki alokacji umożliwiające deduplikację na poziomie bloków to 8 KB, 16 KB oraz 64 KB.*

- Jeśli archiwum jest chronione hasłem

  Wskazówka: *Aby chronić dane archiwum, a jednocześnie zezwolić na ich deduplikację, nie należy zabezpieczać archiwum hasłem, a jedynie zaszyfrować sam skarbiec deduplikacji za pomocą hasła podczas jego tworzenia.*

Bloki dysku, które nie zostały poddane deduplikacji, będą przechowywane w archiwum w taki sam sposób, jak gdyby były przechowywane w skarbcu bez aktywnej funkcji deduplikacji.

Ograniczenia deduplikacji na poziomie plików

Podczas tworzenia kopii zapasowej pliku w archiwum skarbca deduplikacji, w poniższych przypadkach nie następuje deduplikacja pliku:

- Jeśli plik został zaszyfrowany i pole wyboru **Pliki zaszyfrowane zapisz w archiwach w postaci odszyfrowanej** w opcjach tworzenia kopii zapasowych nie jest zaznaczone (domyślnie nie jest zaznaczone)
- Jeśli rozmiar pliku jest mniejszy niż 4 KB
- Jeśli archiwum jest chronione hasłem

Pliki, które nie zostały poddane deduplikacji, będą przechowywane w archiwum w taki sam sposób, jak gdyby były przechowywane w skarbcu bez aktywnej funkcji deduplikacji.

Deduplikacja i strumienie danych NTFS

W systemie plików NTFS z plikiem można skojarzyć jeden lub więcej zestawów danych, zwanych często *alternatywnymi strumieniami danych*.

Podczas tworzenia kopii zapasowej takiego pliku równocześnie kopiowane są wszystkie alternatywne strumienie danych pliku. Jednak strumienie nigdy nie podlegają deduplikacji, nawet po deduplikacji samego pliku.

2.15.7 Uprawnienia zarządzania scentralizowanego

W tej sekcji opisano uprawnienia użytkowników wymagane w celu lokalnego i zdalnego zarządzania komputerem, zarządzania komputerem zarejestrowanym na serwerze zarządzania Acronis Backup & Recovery 10 Management Server oraz uzyskania dostępu do węzła magazynowania Acronis Backup & Recovery 10 Storage Node i zarządzania nim.

Typy połączeń z komputerem zarządzanym

Istnieją dwa typy połączeń z komputerem zarządzanym: połączenie lokalne i połączenie zdalne.

Połączenie lokalne

Połączenie lokalne występuje pomiędzy konsolą zarządzania Acronis Backup & Recovery 10 Management Console na komputerze i agentem Acronis Backup & Recovery 10 Agent, znajdującym się na tym samym komputerze.

Aby ustanowić połączenie lokalne

- Na pasku narzędzi kliknij **Połącz**, a następnie wskaż **Nowe połączenie** i kliknij **Ten komputer**.

Połączenie zdalne

Połączenie zdalne występuje pomiędzy konsolą zarządzania Acronis Backup & Recovery 10 Management Console na komputerze i agentem Acronis Backup & Recovery 10 Agent, znajdującym się na innym komputerze.

Aby ustanowić połączenie zdalne, może być konieczne określenie poświadczeń logowania.

Aby ustanowić połączenie zdalne

1. Na pasku narzędzi kliknij **Połącz**, a następnie wskaż **Nowe połączenie** i kliknij **Zarządzaj komputerem zdalnym**.
2. W obszarze **Komputer** wpisz lub wybierz nazwę i adres IP komputera zdalnego, z którym połączenie ma zostać nawiązane lub kliknij **Przeglądaj**, aby wybrać komputer z listy.
3. Aby określić poświadczenia połączenia, kliknij **Opcje**, a następnie wpisz nazwę użytkownika i hasło odpowiednio w polach **Nazwa użytkownika** i **Hasło**. Jeśli w systemie Windows pole **Nazwa użytkownika** będzie puste, program użyje poświadczeń wykorzystywanych przez konsolę.
4. Aby zapisać hasło dla określonej nazwy użytkownika, zaznacz pole wyboru **Zapisz hasło**. Hasło zostanie zapisane i będzie przechowywane w bezpiecznej lokalizacji na komputerze, na którym działa konsola.

Uprawnienia połączeń lokalnych

Windows

Połączenie lokalne na komputerze z systemem Windows może nawiązać dowolny użytkownik posiadający uprawnienia do lokalnego logowania się na tym komputerze.

Linux

Nawiązanie połączenia lokalnego na komputerze z systemem Linux i zarządzanie takim komputerem wymaga uprawnień użytkownika root.

Aby nawiązać połączenie lokalne jako użytkownik root

1. Po zalogowaniu jako użytkownik root uruchom następujące polecenie:
   ```
   /usr/sbin/acronis_console
   ```
   Lub następujące polecenie:
   ```
   su -c /usr/sbin/acronis_console
   ```
2. Kliknij **Zarządzaj tym komputerem**.

Aby umożliwić uruchamianie konsoli użytkownikowi innemu niż root

- Jako użytkownik root dodaj do pliku **/etc/sudoers** nazwy użytkowników, którym chcesz zezwolić na uruchamianie konsoli, na przykład przy użyciu polecenia **visudo**.

Przestroga: *Po wykonaniu tej procedury użytkownik inny niż root będzie mógł nie tylko uruchamiać konsolę, ale również wykonywać inne działania jako użytkownik root.*

Aby nawiązać połączenie lokalne jako użytkownik inny niż root

1. Upewnij się, że użytkownik root umożliwił uruchamianie konsoli, jak opisano to w poprzedniej procedurze.
2. Uruchom następujące polecenie:
   ```
   sudo /usr/sbin/acronis_console
   ```
3. Kliknij **Zarządzaj tym komputerem**.

Uprawnienia połączeń zdalnych w systemie Windows

Aby nawiązać połączenie zdalne z komputerem z systemem Windows, użytkownik musi należeć do grupy zabezpieczeń Acronis Remote Users na tym komputerze.

Po nawiązaniu połączenia zdalnego użytkownik ma prawa zarządzania na komputerze zdalnym, które opisano w sekcji Prawa użytkownika na komputerze zarządzanym (s. 34).

Uwaga: *Na komputerze zdalnym z systemem Windows Vista, na którym jest włączona usługa kontroli konta użytkownika (UAC) i który nie jest częścią domeny, wyłącznie użytkownik korzystający z wbudowanego konta administratora może tworzyć kopie zapasowe danych i wykonywać operacje zarządzania. Aby obejść to ograniczenie, należy dodać komputer do domeny lub wyłączyć na nim usługę kontroli konta użytkownika (domyślnie jest ona włączona). Tę samą metodę należy zastosować na komputerach z systemami Windows Server 2008 i Windows 7.*

Aby uzyskać informacje o grupach zabezpieczeń Acronis i ich członkach domyślnych, zobacz Grupy zabezpieczeń Acronis (s. 89).

Uprawnienia połączeń zdalnych w systemie Linux

Zdalne połączenia z komputerami z systemem Linux, w tym również nawiązywane przez użytkownika root, są nawiązywane zgodnie z zasadami uwierzytelniania skonfigurowanymi w module Pluggable Authentication Modules for Linux, znanym jako Linux-PAM.

Aby umożliwić działanie zasad uwierzytelniania, zalecamy zainstalowanie najnowszej wersji modułu Linux-PAM dla dystrybucji systemu Linux. Najnowszy stabilny kod źródłowy systemu Linux-PAM jest dostępny na stronie internetowej z kodem źródłowym systemu Linux-PAM.

Zdalne połączenie jako użytkownik root

Zdalne połączenia są nawiązywane przez użytkownika root zgodnie z zasadą uwierzytelniania agenta Acronis, która jest konfigurowana automatycznie podczas instalowania komponentu Acronis Backup & Recovery 10 Agent for Linux, przez utworzenie pliku /etc/pam.d/agentAcronis o następującej zawartości:

```
#%PAM-1.0
auth     required     pam_unix.so
auth     required     pam_succeed_if.so uid eq 0
account  required     pam_unix.so
```

Zdalne połączenie jako użytkownik inny niż root

Ponieważ dostęp do systemu jako użytkownik root powinien być ograniczony, użytkownik root może utworzyć zasadę uwierzytelniania, aby umożliwić zdalne zarządzanie przy użyciu poświadczeń innych niż root.

Poniżej podano dwa przykłady takich zasad.

Uwaga: *W efekcie określeni użytkownicy inni niż root będą mogli zdalnie łączyć się z komputerem tak, jakby mieli uprawnienia użytkownika root. Dobrą praktyką ze względów bezpieczeństwa jest odpowiednie zabezpieczenie kont tych użytkowników przed włamaniem — na przykład przez wymóg używania na nich silnych haseł.*

Przykład 1

Ta zasada uwierzytelniania używa modułu pam_succeed_if i działa w dystrybucjach systemu Linux z jądrem w wersji 2.6 lub nowszej. Zasadę uwierzytelniania działającą z jądrem w wersji 2.4 przedstawiono w następnym przykładzie.

Jako użytkownik root wykonaj następujące czynności:

1. Utwórz konto grupy **Acronis_Trusted**, uruchamiając następujące polecenie:
   ```
   groupadd Acronis_Trusted
   ```
2. Dodaj do grupy **Acronis_Trusted** nazwy użytkowników innych niż root, którym chcesz zezwolić na zdalne łączenie się z komputerem. Aby na przykład dodać do grupy istniejącego użytkownika user_a, uruchom następujące polecenie:
   ```
   usermod -G Acronis_Trusted user_a
   ```
3. Utwórz plik **/etc/pam.d/Acronisagent-trusted** o następującej zawartości:
   ```
   #%PAM-1.0
   auth       required   pam_unix.so
   auth       required   pam_succeed_if.so user ingroup Acronis_Trusted
   account    required   pam_unix.so
   ```

Przykład 2

Powyższa zasada uwierzytelniania może nie działać w dystrybucjach systemu Linux o wersji jądra 2.4 — w tym w systemach Red Hat Linux i VMware® ESX™ 3.5 Upgrade 2, ponieważ moduł pam_succeed_if.so nie jest w nich obsługiwany.

Można wtedy użyć następującej zasady uwierzytelniania.

1. Jako użytkownik root utwórz plik **/etc/pam.d/Acronis_trusted_users**
2. Dodaj do tego pliku nazwy użytkowników niebędących użytkownikami root, którym chcesz zezwolić na zarządzanie komputerem (każda nazwa w osobnym wierszu). Aby na przykład dodać użytkowników uzytk_a, uzytk_b i uzytk_c, dodaj do pliku następujące trzy wiersze:

   ```
   user_a
   user_b
   user_c
   ```

   W razie konieczności dodaj do pliku również użytkownika root.
3. Utwórz plik **/etc/pam.d/Acronisagent-trusted** o następującej zawartości:

   ```
   #%PAM-1.0
   auth     required     pam_unix.so
   auth     required     pam_listfile.so item=user sense=allow
   file=/etc/pam.d/Acronis_trusted_users onerr=fail
   account  required     pam_unix.so
   ```

Grupy zabezpieczeń Acronis

Na komputerze z systemem Windows grupy zabezpieczeń Acronis określają, kto może zdalnie zarządzać komputerem i działać jako administrator serwera Acronis Backup & Recovery 10 Management Server.

Grupy te są tworzone podczas instalowania agentów Acronis Backup & Recovery 10 lub serwera Acronis Backup & Recovery 10 Management Server. Można wówczas określić użytkowników należących do poszczególnych grup.

Agenty Acronis Backup & Recovery 10

Podczas instalowania na komputerze agenta Acronis Backup & Recovery 10 Agent for Windows program tworzy (lub aktualizuje) grupę **Acronis Remote Users**.

Użytkownik należący do tej grupy może zarządzać zdalnie komputerem przy użyciu konsoli Acronis Backup & Recovery 10 Management Console, zgodnie z uprawnieniami do zarządzania opisanymi w sekcji Przywileje użytkowników na zarządzanych komputerach (s. 34).

Domyślnie do tej grupy należą wszyscy członkowie grupy Administratorzy.

Serwer Acronis Backup & Recovery 10 Management Server

Podczas instalowania na komputerze serwera Acronis Backup & Recovery 10 Management Server program tworzy (lub aktualizuje) dwie grupy:

Acronis Centralized Admins

Użytkownik należący do tej grupy jest administratorem serwera zarządzania. Administratorzy serwera zarządzania mogą łączyć się z serwerem zarządzania przy użyciu konsoli Acronis Backup & Recovery 10 Management Console. Mają oni takie same uprawnienia do zarządzania na zarejestrowanych komputerach, jak użytkownicy z uprawnieniami administracyjnymi na tych komputerach — niezależnie od zawartości grup zabezpieczeń Acronis.

Aby nawiązać *zdalne* połączenie z serwerem zarządzania, administrator serwera zarządzania musi również należeć do grupy zdalnych użytkowników Acronis Remote Users.

Żaden użytkownik, nawet należący do grupy Administratorzy, nie może być administratorem serwera zarządzania, jeśli nie należy do grupy administratorów centralnych Acronis Centralized Admins.

Domyślnie do tej grupy należą wszyscy członkowie grupy Administratorzy.

Acronis Remote Users

Użytkownik należący do tej grupy może nawiązywać zdalne połączenie z serwerem zarządzania przy użyciu konsoli Acronis Backup & Recovery 10 Management Console, pod warunkiem, że należy również do grupy administratorów centralnych Acronis Centralized Admins.

Domyślnie do tej grupy należą wszyscy członkowie grupy Administratorzy.

Informacje na temat kontrolera domeny

Jeśli komputer jest kontrolerem domeny Active Directory, nazwy i domyślna zawartość grup zabezpieczeń Acronis są inne:

- Grupy zdalnych użytkowników **Acronis Remote Users** i administratorów centralnych **Acronis Centralized Admins** noszą odpowiednio nazwy *DCNAME* **$ Acronis Remote Users** i *DCNAME* **$ Acronis Centralized Admins**. *DCNAME* oznacza nazwę NetBIOS kontrolera domeny. Po obu stronach każdego znaku dolara występują pojedyncze spacje.
- Zamiast bezpośredniego uwzględnienia nazw wszystkich członków grupy Administratorzy dołączona jest cała grupa Administratorzy.

Wskazówka: *Aby zapewnić odpowiednie nazwy grup, należy zainstalować komponenty Acronis na kontrolerze domeny po jego skonfigurowaniu. Jeśli komponenty będą zainstalowane przed skonfigurowaniem kontrolera domeny, należy ręcznie utworzyć grupy zdalnych użytkowników* DCNAME ***$ Acronis Remote users*** *i administratorów centralnych* DCNAME ***$ Acronis Centralized Admins****, a następnie dodać do nich członków grup Acronis Remote Users i Acronis Centralized Admins.*

Prawa administratora serwera zarządzania

Zwykle administrator serwera zarządzania Acronis Backup & Recovery 10 Management Server działa na komputerze zarejestrowanym w imieniu usługi komputera zarządzanego Acronis Managed Machine Service (znanej również jako usługa Acronis) uruchomionej na tym komputerze i z jej uprawnieniami.

Ewentualnie, tworząc zasady tworzenia kopii zapasowych, administrator serwera zarządzania może wprost określić konto użytkownika, z którego będą wykonywane scentralizowane plany tworzenia kopii zapasowych na komputerach zarejestrowanych. W takim przypadku konto użytkownika musi istnieć na wszystkich komputerach, na których zostaną wdrożone zasady scentralizowane. Nie zawsze jest to metoda skuteczna.

Administratorem serwera zarządzania musi być użytkownik będący członkiem grupy Acronis Centralized Admins (Administratorów centralnych) na komputerze, na którym jest zainstalowany serwer zarządzania.

Uprawnienia użytkownika w węźle magazynowania

Zakres uprawnień użytkownika w węźle magazynowania Acronis Backup & Recovery 10 Storage Node zależy od praw użytkownika na komputerze z zainstalowanym węzłem magazynowania.

Jako członek grupy użytkowników w węźle magazynowania zwykły użytkownik może:

- tworzyć archiwa w dowolnym centralnym skarbcu zarządzanym przez węzeł magazynowania;
- wyświetlać i zarządzać archiwami należącymi do użytkownika.

Użytkownik, który jest członkiem grupy administratorów w węźle magazynowania, może dodatkowo:

- wyświetlać i zarządzać dowolnym archiwum w dowolnym centralnym skarbcu zarządzanym przez węzeł magazynowania;
- tworzyć skarbce centralne do zarządzania przez węzeł magazynowania — pod warunkiem, że użytkownik jest również administratorem serwera zarządzania Acronis Backup & Recovery 10 Management Server;
- zmieniać harmonogram zadania kompaktowania zgodnie z opisem w sekcji Operacje na węzłach magazynowania (s. 363) w pozycji „Zmień harmonogram zadania kompaktowania".

Użytkowników posiadających te dodatkowe uprawnienia nazywa się również administratorami węzła magazynowania.

Zalecenia dotyczące kont użytkowników

Aby zezwolić użytkownikom na dostęp do centralnych skarbców zarządzanych przez węzeł magazynowania, należy dopilnować, aby posiadali oni prawa dostępu do węzła magazynowania za pośrednictwem sieci.

Jeśli komputery użytkowników i komputer z węzłem magazynowania znajdują się w jednej domenie Active Directory, prawdopodobnie nie trzeba wykonywać dalszych kroków: wszyscy użytkownicy są zazwyczaj członkami grupy Użytkownicy domeny i stąd posiadają dostęp do węzła zarządzania.

W przeciwnym razie należy utworzyć konta użytkowników na komputerze z zainstalowanym węzłem magazynowania. Zalecamy utworzenie oddzielnego konta dla każdego użytkownika w celu dostępu do węzła magazynowania, tak aby użytkownicy mieli dostęp wyłącznie do własnych archiwów.

Podczas tworzenia kont, przestrzegaj następujących wytycznych:

- Dodaj do grupy **Administratorzy** konta użytkowników, którzy mają być administratorami węzła magazynowania.
- Dodaj do grupy **Użytkownicy** konta pozostałych użytkowników.

Dodatkowe prawa administratorów komputerów

Użytkownik, który jest członkiem grupy Administratorzy komputera, może wyświetlać i zarządzać dowolnymi archiwami utworzonymi *za pomocą tego komputera* w skarbcu zarządzanym — niezależnie od typu konta użytkownika w węźle magazynowania.

Przykład

Załóżmy, że dwóch użytkowników komputera — użytkownik UserA i użytkownik UserB — wykonują na tym komputerze kopie zapasowe przesyłane do skarbca centralnego zarządzanego przez węzeł magazynowania. W węźle magazynowania użytkownicy mają zwykłe (nie administracyjne) konta — odpowiednio UserA_SN i UserB_SN.

Użytkownik UserA ma zwykle dostęp wyłącznie do archiwów utworzonych przez użytkownika UserA (i należących do UserA_SN), natomiast użytkownik UserB ma dostęp wyłącznie do archiwów utworzonych przez użytkownika UserB (i należących do UserB_SN).

Jednak jeśli użytkownik UserA jest członkiem grupy Administratorzy na komputerze, może on dodatkowo korzystać z dostępu do archiwów utworzonych na tym komputerze przez użytkownika UserB — nawet jeśli użytkownik UserA posiada w węźle magazynowania konto zwykłe.

Prawa dotyczące usług Acronis

Komponenty Acronis Backup & Recovery 10 Agent dla systemu Windows, Acronis Backup & Recovery 10 Management Server i Acronis Backup & Recovery 10 Storage Node działają jako usługi. Podczas instalacji dowolnego z tych komponentów należy określić konto, na którym będzie uruchamiana jego usługa.

Dla każdej usługi można utworzyć specjalne konto użytkownika (zalecane w większości przypadków) albo określić istniejące konto użytkownika lokalnego lub użytkownika domeny, na przykład: .**\UżytkownikLokalny** lub **NazwaDomeny\UżytkownikDomeny**.

W przypadku decyzji o utworzeniu specjalnych kont użytkowników dla usług program utworzy następujące konta użytkowników:

- Dla usługi komponentu Acronis Backup & Recovery 10 Agent dla systemu Windows: **Acronis Agent User**
- Dla usługi serwera Acronis Backup & Recovery 10 Management Server: **AMS User**
- Dla usługi węzła Acronis Backup & Recovery 10 Storage Node: **ASN User**

Nowo utworzone konta otrzymają następujące uprawnienia:

- Do wszystkich trzech kont program przypisze prawo użytkownika **Logowanie jako usługa**.
- Konto użytkownika Acronis Agent User otrzyma uprawnienia **Dostosuj przydziały pamięci dla procesów** i **Zamień token na poziomie procesu**.
- Konta użytkowników Acronis Agent User i ASN User zostaną włączone do grupy **Operatorzy kopii zapasowych**.
- Konto Użytkownik AMS User jest dołączone do grupy **Acronis Centralized Admins**.

Program instalacyjny przypisze powyższe uprawnienia użytkownika do dowolnego istniejącego konta, które zostało określone dla wybranej usługi.

W przypadku decyzji o określeniu dla usługi agenta lub usługi węzła magazynu istniejącego konta użytkownika przed kontynuowaniem instalacji należy sprawdzić, czy dane konto należy do grupy **Operatorzy kopii zapasowych**.

Jeśli dla usługi serwera zarządzania określisz istniejące konto użytkownika, program automatycznie doda to konto do grupy **Acronis Centralized Admins**.

Jeśli komputer należy do domeny Active Directory, upewnij się, że zasady zabezpieczeń domeny nie uniemożliwiają kontom opisanym w tej sekcji (istniejącym lub nowo utworzonym) posiadania wymienionych wyżej praw użytkownika.

Ważne: *Po instalacji nie należy określać innego konta użytkownika dla usługi komponentu. W przeciwnym przypadku komponent może przestać działać.*

Nowo utworzeni użytkownicy uzyskują również dostęp do klucza rejestru HKEY_LOCAL_MACHINE\SOFTWARE\Acronis (zwanego kluczem rejestru Acronis) z następującymi prawami: **zapytanie o wartość**, **ustawianie wartości**, **tworzenie podklucza**, **wyliczanie podkluczy**, **powiadamianie**, **usuwanie** i **kontrola odczytu**.

Dodatkowo dwie usługi Acronis są uruchamiane na koncie systemowym:

- Usługa **Acronis Scheduler2 Service** umożliwia tworzenie harmonogramów zadań komponentów Acronis. Jest uruchamiana na koncie System lokalny i nie można jej uruchomić na innym koncie.

- Usługa **Acronis Remote Agent Service** umożliwia łączność między komponentami Acronis. Jest uruchamiana na koncie Usługa sieciowa i nie można jej uruchomić na innym koncie.

2.15.8 Komunikacja między komponentami programu Acronis Backup & Recovery 10

W tej sekcji opisano sposób komunikowania się ze sobą komponentów programu Acronis Backup & Recovery 10 przy użyciu bezpiecznego uwierzytelniania i szyfrowania.

Ta sekcja zawiera także informacje na temat konfigurowania ustawień komunikacji, wybierania portu sieciowego do komunikacji i zarządzania certyfikatami zabezpieczeń.

Bezpieczna komunikacja

Program Acronis Backup & Recovery 10 zapewnia ochronę danych przesyłanych pomiędzy jego komponentami w sieci lokalnej i sieci granicznej (zwanej również strefą zdemilitaryzowaną, DMZ).

Istnieją dwa mechanizmy, które zapewniają bezpieczną komunikację pomiędzy komponentami programu Acronis Backup & Recovery 10:

- **Bezpieczne uwierzytelnianie** zapewnia bezpieczny transfer certyfikatów potrzebnych do ustanowienia połączenia poprzez wykorzystanie protokołu SSL.
- **Komunikacja zaszyfrowana** umożliwia bezpieczny transfer informacji pomiędzy dowolnymi dwoma komponentami — na przykład agentem Acronis Backup & Recovery 10 Agent i węzłem magazynowania Acronis Backup & Recovery 10 Storage Node — poprzez szyfrowanie przesyłanych danych.

Instrukcje dotyczące konfiguracji bezpiecznego uwierzytelniania i ustawień szyfrowania danych znajdują się w sekcji Konfiguracja opcji komunikacji (s. 94).

Instrukcje dotyczące zarządzania certyfikatami SSL wykorzystywanymi do bezpiecznego uwierzytelniania znajdują się w sekcji Certyfikaty SSL (s. 97).

Uwaga: *Łączność pomiędzy komponentami wcześniejszych produktów Acronis, w tym z rodziny Acronis True Image Echo a komponentami programu Acronis Backup & Recovery 10 jest niemożliwa, niezależnie od ustawień bezpiecznego uwierzytelniania i szyfrowania danych.*

Aplikacje klienckie i serwerowe

W procesie bezpiecznej komunikacji udział biorą dwie strony:

- **Aplikacja kliencka** (klient) to aplikacja, która próbuje nawiązać połączenie.
- **Aplikacja serwerowa** (serwer) to aplikacja, z którą klient próbuje nawiązać połączenie.

Na przykład jeśli konsola Acronis Backup & Recovery 10 Management Console łączy się z agentem Acronis Backup & Recovery 10 na komputerze zdalnym, konsola jest klientem, a agent jest serwerem.

Komponent Acronis może służyć jako aplikacja kliencka, aplikacja serwerowa lub jako oba typy aplikacji, zgodnie z poniższą tabelą.

Nazwa komponentu	Może być klientem	Może być serwerem
Acronis Backup & Recovery 10 Management Console	Tak	Nie
Acronis Backup & Recovery 10 Agent	Tak	Tak

Acronis Backup & Recovery 10 Management Server	Tak	Tak
Acronis Backup & Recovery 10 Storage Node	Tak	Tak
Acronis PXE Server	Nie	Tak
Acronis Backup & Recovery 10 Bootable Agent	Tak	Tak

Konfigurowanie ustawień komunikacji

Ustawienia komunikacji, takie jak szyfrowanie przesyłanych danych, można skonfigurować dla komponentów Acronis Backup & Recovery 10 zainstalowanych na jednym lub większej liczbie komputerów, korzystając z szablonu Acronis Administrative Template. Informacje na temat sposobu ładowania szablonu administracyjnego zawiera sekcja Jak stosować szablon Acronis Administrative Template (s. 378).

Szablon administracyjny zastosowany do pojedynczego komputera definiuje ustawienia komunikacji dla wszystkich komponentów na tym komputerze. Jeśli szablon zostanie zastosowany do domeny lub jednostki organizacyjnej, definiuje ustawienia komunikacji dla wszystkich komponentów na komputerach w tej domenie lub jednostce organizacyjnej.

Aby skonfigurować ustawienia komunikacji

1. Kliknij **Start**, kliknij **Uruchom** i wpisz **gpedit.msc**.
2. W konsoli **Zasady grupy** rozwiń kolejno węzły **Konfiguracja komputera** i **Szablony administracyjne**, a następnie kliknij pozycję Acronis.
3. W panelu Acronis po prawej stronie kliknij dwukrotnie opcję komunikacji, którą chcesz skonfigurować. Szablon administracyjny zawiera następujące opcje (opis poszczególnych opcji znajduje się w dalszej części tego tematu):
   - **porty zdalnego agenta,**
   - **opcje szyfrowania klienta,**
   - **opcje szyfrowania serwera.**
4. Aby nowe ustawienia komunikacji zostały zastosowane, należy ponownie uruchomić wszystkie działające komponenty Acronis, najlepiej uruchamiając ponownie system Windows. Jeśli ponowne uruchomienie nie jest możliwe, wykonaj następujące czynności:
   - Jeśli konsola Acronis Backup & Recovery 10 Management Console jest uruchomiona, zamknij ją i uruchom ponownie.
   - Jeśli uruchomione są inne komponenty programu Acronis, takie jak agent Acronis Backup & Recovery 10 Agent for Windows lub serwer Acronis Backup & Recovery 10 Management Server, uruchom ponownie odpowiednie usługi w przystawce **Usługi** w systemie Windows.

Porty zdalnego agenta,

Określa port, który będzie używany przez komponent do komunikacji przychodzącej i wychodzącej z innymi komponentami programu Acronis.

Wybierz jedno z następujących ustawień:

Nieskonfigurowane

Komponent będzie używać domyślnego numeru portu TCP 9876.

Włączone

Komponent będzie używać określonego portu; wpisz numer portu w polu **Server TCP Port** (Port TCP serwera).

Wyłączone

Analogicznie jak **Nieskonfigurowane**.

Szczegółowe informacje na temat portu sieciowego i sposobu określania go w systemie Linux i środowisku startowym zawiera sekcja Konfiguracja portu sieciowego (s. 96).

Opcje szyfrowania klienta,

Określa, czy przesyłane dane mają być szyfrowane, kiedy komponent służy jako aplikacja kliencka, a także czy należy ufać samopodpisanym certyfikatom SSL.

Wybierz jedno z następujących ustawień:

Nieskonfigurowane

Komponent będzie używać ustawień domyślnych, tzn. będzie używać szyfrowania, jeśli to możliwe, oraz ufać samopodpisanym certyfikatom SSL (patrz poniższa opcja).

Włączone

Szyfrowanie jest włączone. Wybierz jedno z następujących ustawień dla opcji **Szyfrowanie**:

Włączone

Przesyłane dane będą szyfrowane, jeśli szyfrowanie zostało włączone w aplikacji serwerowej. W przeciwnym razie dane nie będą szyfrowane.

Wyłączone

Szyfrowanie jest wyłączone. Nie będzie można nawiązać żadnych połączeń z aplikacją serwerową, która wymaga szyfrowania.

Wymagane

Dane będą przesyłane tylko w przypadku, gdy szyfrowanie zostało włączone w aplikacji serwerowej (patrz sekcja Opcje szyfrowania serwera). Przesyłane dane będą szyfrowane.

Parametry uwierzytelniania

Zaznaczenie pola wyboru **Trust self-signed certificates** (Ufaj samopodpisanym certyfikatom) umożliwi klientowi nawiązanie połączenia z aplikacjami serwerowymi, które używają samopodpisanych certyfikatów, takich jak certyfikaty utworzone podczas instalacji komponentów Acronis Backup & Recovery 10 (patrz sekcja Certyfikaty SSL (s. 97)).

To pole wyboru powinno być zaznaczone, chyba że w danym środowisku używana jest infrastruktura klucza publicznego (PKI).

Wybierz jedno z następujących ustawień dla opcji **Use Agent Certificate Authentication** (Użyj uwierzytelniania certyfikatu agenta):

Nie używaj

Użycie certyfikatów SSL jest wyłączone. Nie będzie można nawiązać żadnych połączeń z aplikacją serwerową, która wymaga użycia certyfikatów SSL.

Use if possible (Użyj, jeśli to możliwe)

Użycie certyfikatów SSL jest włączone. Klient będzie używać certyfikatów SSL, jeśli zostały one włączone w aplikacji serwerowej. W przeciwnym razie certyfikaty SSL nie będą używane.

Always use (Zawsze używaj)

Użycie certyfikatów SSL jest włączone. Połączenie zostanie nawiązane tylko w przypadku, gdy użycie certyfikatów SSL zostało włączone w aplikacji serwerowej.

Wyłączone

Analogicznie jak **Nieskonfigurowane**.

Opcje szyfrowania serwera.

Określa, czy przesyłane dane mają być szyfrowane, kiedy komponent służy jako aplikacja serwerowa.

Wybierz jedno z następujących ustawień:

Nieskonfigurowane

Komponent będzie używać ustawienia domyślnego, tzn. będzie używać szyfrowania, jeśli to możliwe (patrz poniższa opcja).

Włączone

Szyfrowanie jest włączone. Wybierz jedno z następujących ustawień dla opcji **Szyfrowanie**:

Włączone

Przesyłane dane będą szyfrowane, jeśli szyfrowanie zostało włączone w aplikacji klienckiej. W przeciwnym razie dane nie będą szyfrowane.

Wyłączone

Szyfrowanie jest wyłączone. Nie będzie można nawiązać żadnych połączeń z aplikacją kliencką, która wymaga szyfrowania.

Wymagane

Dane będą przesyłane tylko w przypadku, gdy szyfrowanie zostało włączone w aplikacji klienckiej (patrz sekcja Opcje szyfrowania klienta). Przesyłane dane będą szyfrowane.

Parametry uwierzytelniania

Wybierz jedno z następujących ustawień dla opcji **Use Agent Certificate Authentication** (Użyj uwierzytelniania certyfikatu agenta):

Nie używaj

Użycie certyfikatów SSL jest wyłączone. Nie będzie można nawiązać żadnych połączeń z aplikacją kliencką, która wymaga użycia certyfikatów SSL.

Use if possible (Użyj, jeśli to możliwe)

Użycie certyfikatów SSL jest włączone. Serwer będzie używać certyfikatów SSL, jeśli zostały one włączone w aplikacji klienckiej. W przeciwnym razie certyfikaty SSL nie będą używane.

Always use (Zawsze używaj)

Użycie certyfikatów SSL jest włączone. Połączenie zostanie nawiązane tylko w przypadku, gdy użycie certyfikatów SSL zostało włączone w aplikacji klienckiej.

Wyłączone

Analogicznie jak **Nieskonfigurowane**.

Konfiguracja portu sieciowego

Domyślnie komponenty programu Acronis Backup & Recovery 10 korzystają z portu komunikacji sieciowej 9876/TCP. Serwer nasłuchuje ten port pod kątem połączeń przychodzących. Klient Acronis również wykorzystuje ten port jako domyślny. Jeśli użytkownik korzysta z zapory ogniowej innej niż

Zapora systemu Windows, może zostać poproszony podczas instalacji komponentu o potwierdzenie otwarcia portu lub o ręczne jego otwarcie.

W dowolnym momencie po instalacji porty można zmienić według preferowanych wartości lub dla celów bezpieczeństwa. Ta operacja wymaga ponownego uruchomienia agenta Acronis Remote Agent (w systemie Windows) lub usługi Acronis_agent (w systemie Linux).

Po zmianie portu po stronie serwera połącz się z serwerem używając notacji URL <IP_serwera>:<port> lub <nazwa_hosta_serwera>:<port>.

Uwaga: *Jeśli użytkownik korzysta z translatora adresów sieciowych (NAT), port można skonfigurować również za pomocą ustawienia mapowania portu.*

Konfiguracja portu w systemie operacyjnym

Windows

Aby umożliwić zmianę numerów portów, należy załadować i skonfigurować Administrative Template firmy Acronis zgodnie z opisem w sekcji Konfiguracja ustawień komunikacji (s. 94), w części „Porty agenta zdalnego”.

Linux

Określ port w pliku /etc/Acronis/Policies/Agent.config. Uruchom ponownie Acronis_agent daemon.

Konfiguracja portu w środowisku startowym

Tworząc nośnik startowy Acronis, można wstępnie skonfigurować port sieciowy, z którego korzystał będzie agent startowy Acronis Backup & Recovery 10 Bootable Agent. Dostępne są następujące opcje:

- Port domyślny (9876)
- Aktualnie wykorzystywany port
- Nowy port (wprowadź numer portu)

Jeśli nie nastąpiła wstępna konfiguracja portu, agent użyje numeru portu domyślnego.

Certyfikaty SSL

W celu bezpiecznego uwierzytelniania komponenty programu Acronis Backup & Recovery 10 używają certyfikatów Secure Sockets Layer (SSL).

Istnieją dwa rodzaje certyfikatów SSL komponentów:

- **Certyfikaty z podpisem własnym**, na przykład certyfikaty generowane automatycznie podczas instalacji komponentu Acronis
- **Certyfikaty bez podpisu własnego**, na przykład certyfikaty wydawane przez niezależne urzędy certyfikacji, takie jak publiczny urząd certyfikacji VeriSign® lub Thawte™, lub przez urząd certyfikacji przedsiębiorstwa użytkownika

Ścieżka certyfikatu

Wszystkie komponenty Acronis zainstalowane na komputerze i spełniające funkcje serwera aplikacji korzystają z certyfikatu SSL zwanego certyfikatem serwera.

W systemie Windows ścieżka certyfikatu i nazwa pliku certyfikatu serwera określone są w kluczu rejestru `HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\Encryption\Server`. Domyślna ścieżka to %SystemDrive%\Program Files\Common Files\Acronis\Agent.

W przypadku certyfikatów z podpisem własnym odcisk certyfikatu (znany również skrótem) umożliwia przyszłą identyfikację hosta: jeśli klient uprzednio połączył się z serwerem za pomocą certyfikatu z podpisem własnym i próbuje ponownie uzyskać połączenie, serwer sprawdza, czy odcisk certyfikatu jest taki sam jak użyty ostatnim razem.

Certyfikaty z podpisem własnym

Jeśli na komputerach z systemem Windows lokalizacja certyfikatów nie zawiera certyfikatu serwera, program automatycznie wygeneruje certyfikat serwera z podpisem własnym, który zostanie zainstalowany podczas instalacji dowolnego komponentu Acronis z wyjątkiem konsoli Acronis Backup & Recovery 10 Management Console.

Jeśli po wygenerowaniu certyfikatu z podpisem własnym nazwa danego komputera zostanie zmieniona, certyfikatu nie będzie można użyć i należy wygenerować nowy.

Aby wygenerować nowy certyfikat z podpisem własnym

1. Zaloguj się jako członek grupy Administratorzy.
2. W menu **Start** kliknij **Uruchom**, a następnie wpisz: **cmd**
3. Uruchom następujące polecenie (zwracając uwagę na cudzysłów):
   ```
   " (?)%CommonProgramFiles%\Acronis\Utils\acroniscert" (?) --reinstall
   ```
4. Uruchom ponownie system Windows lub aktywne usługi Acronis.

Certyfikaty bez podpisu własnego

Zamiast certyfikatów z podpisem własnym można używać certyfikatów wystawionych przez zaufanych niezależnych wydawców albo utworzonych przez urząd certyfikacji własnego przedsiębiorstwa. Służy do tego narzędzie Acronis Certificate Command-line Utility.

Aby zainstalować certyfikat niezależnego podmiotu

1. Kliknij **Start**, następnie **Uruchom**, a następnie wpisz: **certmgr.msc**
2. W konsoli **Certyfikaty** kliknij dwukrotnie nazwę certyfikatu do zainstalowania.
3. Na karcie **Szczegóły** na liście pól kliknij **Odcisk palca**.
4. Zaznacz i skopiuj wartość pola, zwaną odciskiem certyfikatu — na przykład ciąg **20 99 00 b6 3d 95 57 28 14 0c d1 36 22 d8 c6 87 a4 eb 00 85**
5. W menu **Start** kliknij **Uruchom**, a następnie wpisz poniższy tekst w polu **Otwórz**:
   ```
   " (?)%CommonProgramFiles%\Acronis\Utils\acroniscert.exe" (?) --install " (?)20 99 00 b6 3d 95 57 28 14 0c d1 36 22 d8 c6 87 a4 eb 00 85" (?)
   ```
   (Zwróć uwagę na cudzysłowy. Zastąp ten przykładowy odcisk wartością skopiowaną z certyfikatu).

3 Opcje

Ta sekcja obejmuje opcje programu Acronis Backup & Recovery 10, które można skonfigurować przy użyciu graficznego interfejsu użytkownika (GUI). Zawartość tej sekcji dotyczy zarówno autonomicznej, jak i zaawansowanych wersji programu Acronis Backup & Recovery 10.

3.1 Opcje konsoli

Opcje konsoli określają sposób przedstawiania informacji w graficznym interfejsie użytkownika programu Acronis Backup & Recovery 10.

Aby uzyskać dostęp do opcji konsoli, należy wybrać z górnego menu kolejno: **Opcje > Konsola**.

3.1.1 Strona początkowa

Ta opcja określa, czy po połączeniu konsoli z zarządzanym komputerem lub serwerem zarządzania ma być wyświetlany ekran **Witamy** czy też **Pulpit nawigacyjny**.

Ustawienie wstępne: ekran **Witamy**.

Aby dokonać wyboru, zaznacz lub anuluj zaznaczenie pola wyboru obok opcji **Gdy konsola zostanie podłączona do komputera, pokaż widok Pulpit nawigacyjny**.

Tę opcję można również skonfigurować na ekranie **Witamy**. Po zaznaczeniu pola wyboru **Po uruchomieniu wyświetlaj pulpit nawigacyjny zamiast bieżącego widoku** na ekranie **Witamy** powyższe ustawienie zostanie odpowiednio zaktualizowane.

3.1.2 Komunikaty wyskakujące

Informacje na temat zadań wymagających działania

Ta opcja jest uwzględniana, gdy konsola jest połączona z komputerem zarządzanym lub serwerem zarządzania.

Określa ona, czy w przypadku wystąpienia jednego lub kilku zadań wymagających działania użytkownika mają być wyświetlane komunikaty wyskakujące. W tym oknie można podjąć jedną decyzję dla wszystkich zadań, na przykład potwierdzić ponowne uruchomienie lub podjąć ponowną próbę po zwolnieniu miejsca na dysku. Dopóki co najmniej jedno działanie będzie wymagało działania użytkownika, można w dowolnym momencie otworzyć to okno w **Pulpicie nawigacyjnym** komputera zarządzanego. Można również sprawdzić stan wykonywania zadań w widoku **Zadania** i określić decyzje dla poszczególnych zadań w panelu **Informacje**.

Ustawienie wstępne: **Włączone**.

Aby dokonać wyboru, należy zaznaczyć lub anulować zaznaczenie pola wyboru **Wyświetl okno „Zadania wymagają działania użytkownika”**.

Informacje na temat wyników wykonania zadania

Ta opcja jest uwzględniana tylko wtedy, gdy konsola jest połączona z komputerem zarządzanym.

Określa ona, czy mają być wyświetlane komunikaty wyskakujące informujące o wyniku wykonania zadania: zakończone pomyślnie, zakończone niepomyślnie lub pomyślnie z ostrzeżeniami. Gdy wyświetlanie komunikatów wyskakujących jest wyłączone, można sprawdzić stan i wynik wykonania zadania w widoku **Zadania**.

Ustawienie wstępne: **Włączone** dla wszystkich wyników.

Aby określić ustawienie dla poszczególnych wyników, (zakończone pomyślnie, zakończone niepomyślnie lub pomyślnie z ostrzeżeniami), należy zaznaczyć lub anulować zaznaczenie pola wyboru obok odpowiedniej opcji.

3.1.3 Alerty związane z czasem

Ostatnia kopia zapasowa

Ta opcja jest uwzględniana, gdy konsola jest połączona z komputerem zarządzanym (s. 423) lub serwerem zarządzania (s. 427).

Określa ona, czy ma być wyświetlany alert w przypadku, gdy na danym komputerze od pewnego czasu nie została utworzona kopia zapasowa. Można określić czas, który jest krytyczny dla użytkownika.

Ustawienie wstępne: alert w przypadku, gdy ostatnia kopia zapasowa na komputerze została pomyślnie utworzona ponad **5 dni** temu.

Alert jest wyświetlany w sekcji **Alerty** na **Pulpicie nawigacyjnym**. Gdy konsola jest połączona z serwerem zarządzania, to ustawienie określa również schemat kolorów dla wartości w kolumnie **Ostatnia kopia zapasowa** dla każdego komputera.

Ostatnie połączenie

Ta opcja jest uwzględniana gdy konsola jest połączona z serwerem zarządzania lub z zarejestrowanym komputerem (s. 423).

Określa ona, czy ma być wyświetlany alert w przypadku, gdy przez pewien czas nie zostanie nawiązane połączenie pomiędzy komputerem zarejestrowanym a serwerem zarządzania, co oznacza, że komputer może nie być centralnie zarządzany (na przykład w przypadku błędu połączenia sieciowego z tym komputerem). Można skonfigurować okres uważany za krytyczny.

Ustawienie wstępne: alert jest wyświetlany, gdy ostatnie połączenie komputera z serwerem zarządzania nastąpiło ponad **5 dni** temu.

Alert jest wyświetlany w sekcji **Alerty** na **Pulpicie nawigacyjnym**. Gdy konsola jest połączona z serwerem zarządzania, to ustawienie określa również schemat kolorów dla wartości w kolumnie **Ostatnie połączenie** dla każdego komputera.

3.1.4 Liczba zadań

Ta opcja jest uwzględniana tylko wtedy, gdy konsola jest połączona z serwerem zarządzania.

Określa ona, ile zadań może być wyświetlanych jednocześnie w widoku **Zadania**. W celu ograniczenia liczby wyświetlanych zadań można również użyć filtrów dostępnych w widoku **Zadania**.

Ustawienie wstępne: **400**. Zakres regulacji: **20**-**500**.

Aby dokonać wyboru, należy wybrać odpowiednią wartość z menu rozwijanego **Liczba zadań**.

3.1.5 Czcionki

Ta opcja jest uwzględniana, gdy konsola jest połączona z komputerem zarządzanym lub serwerem zarządzania.

Określa ona czcionki używane w graficznym interfejsie użytkownika programu Acronis Backup & Recovery 10. Ustawienie **Menu** dotyczy menu rozwijanego i kontekstowego. Ustawienie **Aplikacja** dotyczy pozostałych elementów interfejsu.

Ustawienie wstępne: **Domyślna systemowa** czcionka zarówno dla menu, jak i elementów interfejsu aplikacji.

Aby dokonać wyboru, należy wybrać czcionkę z odpowiedniego pola kombi i ustawić jej właściwości. Wygląd czcionki można sprawdzić, klikając przycisk po prawej stronie.

3.2 Opcje serwera zarządzania

Opcje serwera zarządzania umożliwiają dostosowanie zachowania serwera Acronis Backup & Recovery 10 Management Server.

Aby uzyskać dostęp do opcji serwera zarządzania, podłącz konsolę do serwera, a następnie wybierz polecenia **Opcje > Opcje serwera zarządzania** z górnego menu.

3.2.1 Poziom dziennika

Ta opcja określa, czy serwer zarządzania ma gromadzić zdarzenia z dzienników na komputerach zarejestrowanych w dzienniku centralnym zapisanym w dedykowanej bazie danych i dostępnym w widoku **Dziennik**. Można ustawić opcję dla wszystkich zdarzeń jednocześnie lub wybrać typy zdarzeń, które mają być gromadzone. W przypadku całkowitego wyłączenia gromadzenia zdarzeń z dzienników w dzienniku centralnym będzie znajdował się wyłącznie dziennik serwera zarządzania.

Ustawienie wstępne: **Zbieraj dzienniki** — **Wszystkie zdarzenia**.

W celu określenia typów gromadzonych zdarzeń należy użyć pola kombi **Typy rejestrowanych zdarzeń**:

- **Wszystkie zdarzenia** — w dzienniku centralnym rejestrowane są wszystkie zdarzenia (informacje, ostrzeżenia i błędy), które wystąpiły na wszystkich komputerach zarejestrowanych na serwerze zarządzania
- **Błędy i ostrzeżenia** — w dzienniku centralnym rejestrowane są ostrzeżenia i błędy
- **Tylko błędy** — w dzienniku centralnym rejestrowane są tylko błędy

Aby wyłączyć gromadzenie zdarzeń z dzienników, należy anulować zaznaczenie pola wyboru **Zbieraj dzienniki**.

3.2.2 Reguły czyszczenia dziennika

Ta opcja określa sposób czyszczenia centralnego dziennika zdarzeń przechowywanego w bazie danych raportowania serwera zarządzania.

Opcja definiuje maksymalny rozmiar bazy danych raportowania.

Ustawienie wstępne: **Maksymalny rozmiar dziennika: 1 GB**. **Podczas czyszczenia zachowaj 95% maksymalnego rozmiaru dziennika**.

Po włączeniu tej opcji program będzie co 100 wpisów dziennika porównywał jego bieżący rozmiar z rozmiarem maksymalnym. Gdy maksymalny rozmiar dziennika zostanie przekroczony, program usunie najstarsze wpisy. Można wybrać liczbę zachowywanych wpisów dziennika. Ustawienie domyślne 95% oznacza zachowanie większości dziennika. Ustawienie minimalne 1% oznacza praktycznie wyczyszczenie dziennika.

Nawet przy usuniętym limicie rozmiaru dziennika rejestrowanie zdarzeń w bazie danych SQL Server Express zostanie przerwane, gdy dziennik osiągnie rozmiar 4 GB. Wynika to z obowiązującego w programie SQL Express Edition limitu rozmiaru bazy danych wynoszącego 4 GB. Jeśli chcesz maksymalnie wykorzystać pojemność bazy danych SQL Express, ustaw maksymalny rozmiar dziennika na około 3,8 GB.

Parametr ten można także ustawić za pomocą szablonu Acronis Administrative Template (s. 382).

3.2.3 Śledzenie zdarzeń

Serwer zarządzania można skonfigurować tak, aby rejestrował zdarzenia w dzienniku zdarzeń aplikacji systemu Windows, a nie tylko we własnym dzienniku.

Serwer zarządzania można skonfigurować tak, aby wysyłał obiekty SNMP (Simple Network Management Protocol) do określonego menedżera SNMP.

Dziennik zdarzeń systemu Windows

Ta opcja określa, czy serwer zarządzania musi rejestrować zdarzenia własnego dziennika w rejestrze zdarzeń aplikacji systemu Windows (aby wyświetlić ten dziennik, należy uruchomić plik **eventvwr.exe** lub wybrać polecenia **Panel sterowania > Administrative tools (Narzędzia administracyjne) > Event Viewer (Podgląd zdarzeń)**). Zdarzenia do rejestrowania można filtrować.

Wstępnie ustawiona wartość: **Wyłączone**.

Aby włączyć tę opcję, zaznacz pole wyboru **Rejestruj zdarzenia**.

Pole wyboru **Typy rejestrowanych zdarzeń** umożliwia filtrowanie zdarzeń rejestrowanych w dzienniku zdarzeń aplikacji systemu Windows:

- **Wszystkie zdarzenia** — wszystkie zdarzenia (informacje, ostrzeżenia i błędy);
- **Błędy i ostrzeżenia;**
- **Tylko błędy**.

Aby wyłączyć tę opcję, anuluj zaznaczenie pola wyboru **Rejestruj zdarzenia**.

Powiadomienia SNMP

Ta opcja określa, czy serwer zarządzania musi wysyłać zdarzenia własnego dziennika do określonych menedżerów SNMP (Simple Network Management Protocol). Można wybrać typy zdarzeń, które będą wysyłane.

Aby uzyskać szczegółowe informacje na temat programu Acronis Backup & Recovery 10, zobacz „Obsługa SNMP (s. 59)”.

Ustawienie wstępne: **Wyłączone**.

Aby skonfigurować wysyłanie komunikatów SNMP

1. Zaznacz pole wyboru **Wysyłaj wiadomości do serwera SNMP**.

2. Określ odpowiednie opcje:
   - **Typy wysyłanych zdarzeń** — wybierz typy zdarzeń: **Wszystkie zdarzenia**, **Błędy i ostrzeżenia** lub **Tylko błędy**.
   - **Nazwa/adres IP serwera** — wpisz nazwę lub adres IP hosta, na którym uruchomiona jest aplikacja zarządzająca SNMP, do której chcesz wysyłać komunikaty.
   - **Społeczność** — wpisz nazwę społeczności SNMP, do której należy host z aplikacją zarządzającą SNMP oraz komputer wysyłający. Typowe ustawienie to „public" („publiczna").

   Kliknij **Wyślij wiadomość próbną**, aby sprawdzić, czy ustawienia są poprawne.

Aby wyłączyć wysłanie komunikatów SNMP, wyczyść pole wyboru **Wysyłaj wiadomości do serwera SNMP**.

Komunikaty są wysyłane przy użyciu protokołu UDP.

3.2.4 Poświadczenia umożliwiające uzyskanie dostępu do domeny

Ta opcja określa nazwę użytkownika i hasło stosowane przez serwer zarządzania w celu uzyskania dostępu do domeny.

Ustawienie wstępne: Brak poświadczeń

Podczas pracy z grupą dynamiczną opartą na kryterium (s. 350) **Jednostka organizacyjna** serwer zarządzania potrzebuje poświadczeń umożliwiających uzyskanie dostępu do domeny. Jeśli tworzysz taką grupę i omawiana opcja nie zawiera poświadczeń, program wyświetli monit o ich podanie i zapisze je w tej opcji.

Wystarczy określić poświadczenia użytkownika należącego w domenie do grupy **Użytkownicy domeny**.

3.2.5 Acronis WOL Proxy

Ta opcja działa w połączeniu z zaawansowanym ustawieniem harmonogramu **Użyj Wake-On-LAN** (s. 195). Użyj tej opcji, jeśli serwer zarządzania w celu utworzenia kopii zapasowej musi wznowić pracę komputerów znajdujących się w innej podsieci.

Gdy zaplanowana operacja ma się zacząć, serwer zarządzania wysyła tzw. magiczne pakiety służące do wznowienia pracy odpowiednich komputerów. (Magiczny pakiet zawiera 16 następujących jedna po drugiej kopii adresu MAC karty NIC odbiorcy). Zainstalowany w drugiej podsieci program Acronis WOL Proxy przenosi pakiety do komputerów znajdujących się w tej podsieci.

Ustawienie wstępne: **Wyłączone**.

Aby włączyć tę opcję:

1. Zainstaluj program Acronis WOL Proxy na dowolnym serwerze w podsieci obejmującej komputery, których pracę chcesz wznawiać. Serwer musi zapewniać nieprzerwaną dostępność usług. Przy wielu podsieciach zainstaluj program Acronis WOL Proxy w każdej podsieci, w której chcesz używać funkcji Wake-On-LAN.
2. Włącz program **Acronis WOL Proxy** w **opcjach serwera zarządzania** w następujący sposób:
   a. Zaznacz pole wyboru **Użyj następujących proxy**.
   b. Kliknij **Dodaj** i wprowadź nazwę lub adres IP komputera z zainstalowanym programem Acronis WOL Proxy. Podaj poświadczenia dla tego komputera.
   c. Powtórz ten krok, jeśli jest zainstalowanych kilka programów Acronis WOL Proxy.

3. Podczas planowania zasad tworzenia kopii zapasowych włącz ustawienie **Użyj Wake-On-LAN**.

Serwery proxy można również usuwać z listy. Pamiętaj o tym, że każda zmiana tej opcji ma wpływ na cały serwer zarządzania. Po usunięciu serwera proxy z listy funkcja Wake-On-LAN w odpowiedniej podsieci zostanie wyłączona we wszystkich zasadach, w tym także w zasadach już zastosowanych.

3.2.6 Opcje ochrony maszyny wirtualnej

Te opcje pozwalają zdefiniować zachowanie serwera zarządzania dotyczące tworzenia kopii zapasowych i odzyskiwania maszyn wirtualnych znajdujących się na serwerach wirtualizacji.

Integracja VMware vCenter

Ta opcja określa, czy na serwerze zarządzania mają być wyświetlane maszyny wirtualne zarządzane przez serwer VMware vCenter Server oraz czy ma być wyświetlany ich status.

Integracja jest dostępna we wszystkich zaawansowanych wersjach produktu Acronis Backup & Recovery 10. Nie jest wymagana licencja wersji Virtual Edition. Na serwerze vCenter Server nie trzeba instalować żadnego oprogramowania.

Po stronie serwera zarządzania

Gdy integracja jest włączona, w interfejsie graficznym serwera zarządzania w sekcji **Nawigacja** > **Maszyny wirtualne** znajduje się widok **Maszyny wirtualne i szablony**.

Z perspektywy serwera zarządzania jest to dynamiczna grupa maszyn wirtualnych. Nazwa grupy odpowiada nazwie lub adresowi IP serwera vCenter Server, zależnie od informacji określonej podczas konfigurowania integracji. Zawartość grupy jest synchronizowana z serwerem vCenter Server i nie może być zmieniana po stronie serwera zarządzania. W razie występowania sporadycznych niespójności kliknij grupę prawym przyciskiem myszy i wybierz **Odśwież**.

Maszyny wirtualne zarządzane przez serwer vCenter Server znajdują się także w grupie **Wszystkie maszyny wirtualne**. Można przeglądać właściwości i stan zasilania maszyn wirtualnych, tworzyć grupy maszyn oraz dodawać maszyny do istniejących grup.

Utworzenie kopii zapasowej maszyny wirtualnej i jej odzyskanie jest możliwe tylko w przypadku, gdy na hoście maszyny wirtualnej został wdrożony (s. 355) komponent Acronis Backup & Recovery 10 Agent dla ESX/ESXi. W przeciwnym razie takie maszyny są wyświetlane jako niemożliwe do zarządzania (wyszarzone).

Po wdrożeniu agenta na hoście ESX/ESXi (wymaga to licencji programu Acronis Backup & Recovery 10 Advanced Server Virtual Edition) maszyny wirtualne z tego hosta będą gotowe do stosowania zasad tworzenia kopii zapasowych oraz do tworzenia pojedynczych kopii. Takie maszyny są wyświetlane jako możliwe do zarządzania.

*Jeśli w systemie-gościu jest zainstalowany agent dla systemu Windows lub dla systemu Linux, ale na jego hoście nie ma agenta dla ESX/ESXi, w sekcji **Maszyny wirtualne** dana maszyna wirtualna jest wyświetlana jako niemożliwa do zarządzania. Taką maszyną należy zarządzać tak jak komputerem fizycznym.*

Po stronie serwera vCenter Server

Gdy integracja jest włączona, serwer vCenter Server przechowuje i wyświetla informacje o dacie i powodzeniu operacji tworzenia kopii zapasowych poszczególnych maszyn wirtualnych. Te same informacje są wyświetlane w kolumnach **Stan** i **Ostatnia kopia zapasowa** na serwerze zarządzania.

Stan kopii zapasowej — najpoważniejszy status wszystkich planów i zasad tworzenia kopii zapasowych na maszynie. Aby uzyskać więcej informacji, zobacz „Statusy planu tworzenia kopii zapasowych” (s. 206) i „Status zasad na komputerze (s. 79)”.

Ostatnia kopia zapasowa — czas od ostatniego pomyślnego utworzenia kopii zapasowej.

Informacje te można wyświetlić w podsumowaniu maszyny wirtualnej (**Podsumowanie** > **Adnotacje**) lub na karcie **Maszyny wirtualne** dla każdego hosta, centrum danych, folderu lub całego serwera vCenter Server (na przykład **Widok** > **Inwentaryzacja** > **Hosty i klastry** > wybierz host > **Maszyny wirtualne**).

3.2.7 Serwer proxy kopii zapasowej online

Ta opcja jest dostępna tylko w przypadku połączenia z magazynem Acronis Online Backup Storage za pośrednictwem Internetu.

Ta opcja określa, czy serwer zarządzania ma łączyć się z Internetem za pośrednictwem serwera proxy.

Uwaga: *Funkcja Acronis Backup & Recovery 10 Online obsługuje wyłącznie serwery proxy HTTP i HTTPS.*

Ustawienia proxy agenta i serwera zarządzania są konfigurowane oddzielnie, nawet jeśli agent i serwer są zainstalowane na tym samym komputerze.

Aby skonfigurować ustawienia serwera proxy

1. Zaznacz pole wyboru **Użyj serwera proxy**.
2. W polu **Adres** określ nazwę sieciową lub adres IP serwera proxy — na przykład: **proxy.example.com** lub **192.168.0.1**
3. W polu **Port** określ numer portu serwera proxy — na przykład: **80**
4. Jeśli serwer proxy wymaga uwierzytelniania, określ poświadczenia w polach **Nazwa użytkownika** i **Hasło**.
5. Aby sprawdzić poprawność ustawień serwera proxy, kliknij **Sprawdź połączenie**.

3.3 Opcje komputera

Opcje komputera określają ogólne zachowanie wszystkich agentów Acronis Backup & Recovery 10 działających na zarządzanym komputerze, w związku z czym są one odrębne dla każdego komputera.

Aby uzyskać dostęp do opcji komputera, należy połączyć konsolę z zarządzanym komputerem, a następnie wybrać z górnego menu kolejno: **Opcje > Opcje komputera**.

3.3.1 Zarządzanie komputerem

Ta opcja określa, czy komputer ma być zarządzany centralnie przez serwer zarządzania Acronis Backup & Recovery 10 Management Server.

Aby móc używać tej opcji, należy zalogować się jako członek grupy **Administratorzy** na komputerze.

Komputer można zarejestrować na serwerze zarządzania podczas instalowania agenta programu Acronis Backup & Recovery 10. Jeśli komputer nie jest zarejestrowany, wybranie opcji **Zarządzanie scentralizowane** spowoduje zainicjowanie rejestracji (s. 427). Komputer można również dodać do serwera zarządzania po stronie samego serwera. Każda z tych trzech metod rejestracji wymaga uprawnień administratora serwera.

Wybranie na zarejestrowanym komputerze opcji **Zarządzanie autonomiczne** spowoduje wstrzymanie jego komunikacji z serwerem. Na serwerze zarządzania komputer jest wyświetlany jako **Wycofany**. Administrator serwera zarządzania może usunąć komputer z serwera lub zarejestrować go ponownie.

Ustawienie wstępne: **Zarządzanie autonomiczne**.

Aby na komputerze skonfigurować zarządzanie scentralizowane:

1. Wybierz **Zarządzanie scentralizowane**.
2. Określ dane w obszarze **Serwer zarządzania (IP/nazwa)**.
3. Po wyświetleniu monitu określ nazwę użytkownika i hasło administratora serwera zarządzania.
4. W polu **Adres rejestracji komputera** wybierz sposób rejestracji serwera zarządzania: wg jego nazwy (sposób zalecany) lub jego adresu IP.
5. Kliknij **OK**. Komputer zostanie zarejestrowany na serwerze zarządzania.

Aby wyłączyć zarządzanie scentralizowane, należy wybrać **Zarządzanie autonomiczne**.

3.3.2 Śledzenie zdarzeń

Zdarzenia z dzienników generowane przez agenty można zduplikować na komputerze zarządzanym, w dzienniku zdarzeń aplikacji systemu Windows. Można także przesłać zdarzenia do określonych menedżerów SNMP. Jeśli opcje śledzenia zdarzeń nie zostaną zmodyfikowane w żadnym innym miejscu, ustawienia będą obowiązywały dla każdego lokalnego planu utworzenia kopii zapasowej i każdego zadania utworzonego na komputerze.

Określone tutaj ustawienia można zastąpić w przypadku zdarzeń występujących podczas tworzenia kopii zapasowych lub odzyskiwania, w sekcji Domyślne opcje tworzenia kopii zapasowej i odzyskiwania (s. 109). W takim przypadku określone tutaj ustawienia będą uwzględniane w przypadku operacji innych niż tworzenie kopii zapasowych i odzyskiwanie, na przykład podczas sprawdzania poprawności archiwum lub czyszczenia.

Podczas tworzenia planu tworzenia kopii zapasowych lub zadania odzyskiwania można również zastąpić ustawienia określone w domyślnych opcjach tworzenia kopii zapasowej i odzyskiwania. Uzyskane w ten sposób ustawienia będą dotyczyły konkretnego planu lub zadania.

Dziennik zdarzeń systemu Windows

Ta opcja jest uwzględniana tylko w systemach operacyjnych Windows.

Jest ona niedostępna podczas pracy z nośnikiem startowym.

Ta opcja określa, czy agenty działające na komputerze zarządzanym muszą rejestrować zdarzenia w dzienniku zdarzeń aplikacji systemu Windows (aby wyświetlić ten dziennik, uruchom program **eventvwr.exe** lub wybierz kolejno: **Panel sterowania > Narzędzia administracyjne > Podgląd zdarzeń**). Zarejestrowane zdarzenia można filtrować.

Określone tutaj ustawienia można zastąpić w przypadku zdarzeń występujących podczas tworzenia kopii zapasowych lub odzyskiwania, w sekcji Domyślne opcje tworzenia kopii zapasowej i odzyskiwania (s. 109). W takim przypadku określone tutaj ustawienia będą uwzględniane w przypadku operacji innych niż tworzenie kopii zapasowych i odzyskiwanie, na przykład podczas sprawdzania poprawności archiwum lub czyszczenia.

Podczas tworzenia planu tworzenia kopii zapasowych lub zadania odzyskiwania można również zastąpić ustawienia określone w domyślnych opcjach tworzenia kopii zapasowej i odzyskiwania. Uzyskane w ten sposób ustawienia będą dotyczyły konkretnego planu lub zadania.

Wstępnie ustawiona wartość: **Wyłączone**.

Aby włączyć tę opcję, zaznacz pole wyboru **Rejestruj zdarzenia**.

Pole wyboru **Typy rejestrowanych zdarzeń** umożliwia filtrowanie zdarzeń rejestrowanych w dzienniku zdarzeń aplikacji systemu Windows:

- **Wszystkie zdarzenia** — wszystkie zdarzenia (informacje, ostrzeżenia i błędy);
- **Błędy i ostrzeżenia;**
- **Tylko błędy**.

Aby wyłączyć tę opcję, anuluj zaznaczenie pola wyboru **Rejestruj zdarzenia**.

Powiadomienia SNMP

Ta opcja jest uwzględniana w systemach operacyjnych Windows i Linux.

Jest ona niedostępna podczas pracy z nośnikiem startowym.

Ta opcja określa, czy agenty działające na komputerze zarządzanym muszą wysyłać zdarzenia z dziennika do określonych menedżerów Simple Network Management Protocol (SNMP). Można wybrać typy wysyłanych zdarzeń.

Określone tutaj ustawienia można zastąpić w przypadku zdarzeń występujących podczas tworzenia kopii zapasowych lub odzyskiwania, w sekcji Domyślne opcje tworzenia kopii zapasowej i odzyskiwania (s. 109). W takim przypadku określone tutaj ustawienia będą uwzględniane w przypadku operacji innych niż tworzenie kopii zapasowych i odzyskiwanie, na przykład podczas sprawdzania poprawności archiwum lub czyszczenia.

Podczas tworzenia planu tworzenia kopii zapasowych lub zadania odzyskiwania można również zastąpić ustawienia określone w domyślnych opcjach tworzenia kopii zapasowej i odzyskiwania. Uzyskane w ten sposób ustawienia będą dotyczyły konkretnego planu lub zadania.

Aby uzyskać szczegółowe informacje na temat programu Acronis Backup & Recovery 10, zobacz „Obsługa SNMP (s. 59)”.

Ustawienie wstępne: **Wyłączone**.

Aby skonfigurować wysyłanie komunikatów SNMP

1. Zaznacz pole wyboru **Wysyłaj wiadomości do serwera SNMP**.
2. Określ odpowiednie opcje:
   - **Typy wysyłanych zdarzeń** — wybierz typy zdarzeń: **Wszystkie zdarzenia**, **Błędy i ostrzeżenia** lub **Tylko błędy**.
   - **Nazwa/adres IP serwera** — wpisz nazwę lub adres IP hosta, na którym uruchomiona jest aplikacja zarządzająca SNMP, do której chcesz wysyłać komunikaty.
   - **Społeczność** — wpisz nazwę społeczności SNMP, do której należy host z aplikacją zarządzającą SNMP oraz komputer wysyłający. Typowe ustawienie to „public” („publiczna”).

   Kliknij **Wyślij wiadomość próbną**, aby sprawdzić, czy ustawienia są poprawne.

Aby wyłączyć wysłanie komunikatów SNMP, wyczyść pole wyboru **Wysyłaj wiadomości do serwera SNMP**.

Komunikaty są wysyłane przy użyciu protokołu UDP.

Następna sekcja zawiera dodatkowe informacje na temat Konfigurowanie usług SNMP na komputerze odbierającym (s. 108).

Konfigurowanie usług SNMP na komputerze odbierającym

Windows

Aby zainstalować usługę SNMP na komputerze z systemem Windows:

1. **Start > Panel sterowania > Dodaj lub usuń programy > Dodaj/Usuń składniki systemu Windows.**
2. Wybierz **Narzędzia zarządzania i monitorowania**.
3. Kliknij **Szczegóły**.
4. Zaznacz pole wyboru **Protokół Simple Network Management Protocol**.
5. Kliknij **OK**.

Może zostać wyświetlony monit o plik lmmib2.dll, który znajduje się na płycie instalacyjnej systemu operacyjnego.

Linux

W celu odbierania komunikatów SNMP na komputerze z systemem Linux należy zainstalować pakiet net-snmp (w przypadku dystrybucji RHEL i SUSE) lub snmpd (w przypadku dystrybucji Debian).

Protokół SNMP można skonfigurować przy użyciu polecenia **snmpconf**. Domyślne pliki konfiguracyjne znajdują się w katalogu /etc/snmp:

- /etc/snmp/snmpd.conf — plik konfiguracyjny agenta SNMP Net-SNMP,
- /etc/snmp/snmptrapd.conf — plik konfiguracyjny demona pułapki Net-SNMP.

3.3.3 Reguły czyszczenia dziennika

Ta opcja określa sposób czyszczenia dziennika agenta programu Acronis Backup & Recovery 10.

Opcja definiuje maksymalny rozmiar folderu z dziennikiem agenta (w systemach Windows XP/2003: %ALLUSERSPROFILE%\Application Data\Acronis\BackupAndRecovery\MMS\LogEvents).

Ustawienie wstępne: **Maksymalny rozmiar dziennika: 1 GB**. **Podczas czyszczenia zachowaj 95% maksymalnego rozmiaru dziennika**.

Po włączeniu tej opcji program będzie co 100 wpisów dziennika porównywał jego bieżący rozmiar z rozmiarem maksymalnym. Gdy maksymalny rozmiar dziennika zostanie przekroczony, program usunie najstarsze wpisy. Można wybrać liczbę zachowywanych wpisów dziennika. Ustawienie domyślne 95% oznacza zachowanie większości dziennika. Ustawienie minimalne 1% oznacza praktycznie wyczyszczenie dziennika.

Parametr ten można także ustawić za pomocą szablonu Acronis Administrative Template (s. 387).

3.3.4 Serwer proxy kopii zapasowej online

Ta opcja jest dostępna tylko w przypadku tworzenia kopii zapasowej oraz odzyskiwania jej z magazynu Acronis Online Backup Storage za pośrednictwem Internetu.

Ta opcja określa, czy agent Acronis ma łączyć się z Internetem za pośrednictwem serwera proxy.

Uwaga: *Funkcja Acronis Backup & Recovery 10 Online obsługuje wyłącznie serwery proxy HTTP i HTTPS.*

Aby skonfigurować ustawienia serwera proxy

1. Zaznacz pole wyboru **Użyj serwera proxy**.

2. W polu **Adres** określ nazwę sieciową lub adres IP serwera proxy — na przykład: **proxy.example.com** lub **192.168.0.1**
3. W polu **Port** określ numer portu serwera proxy — na przykład: **80**
4. Jeśli serwer proxy wymaga uwierzytelniania, określ poświadczenia w polach **Nazwa użytkownika** i **Hasło**.
5. Aby sprawdzić poprawność ustawień serwera proxy, kliknij **Sprawdź połączenie**.

Jeżeli nie znasz ustawień serwera proxy, skontaktuj się z administratorem sieci lub usługodawcą internetowym w celu uzyskania pomocy.

Możesz także posłużyć się ustawieniami z konfiguracji przeglądarki internetowej. Oto informacje ułatwiające odnalezienie ich w trzech popularnych przeglądarkach.

- **Microsoft Internet Explorer.** W menu **Narzędzia** kliknij **Opcje internetowe**. Na karcie **Połączenia** kliknij **Ustawienia sieci LAN**.
- **Mozilla Firefox.** W menu **Narzędzia** kliknij **Opcje**, a następnie kliknij **Zaawansowane**. Na karcie **Sieć** w obszarze **Połączenie** kliknij **Ustawienia**.
- **Google Chrome.** W oknie **Opcje** kliknij **Dla zaawansowanych**. W obszarze **Sieć** kliknij **Zmień ustawienia proxy**.

3.3.5 Program jakości obsługi klienta

Ta opcja określa, czy komputer zostanie objęty Programem jakości obsługi klienta firmy Acronis (ACEP).

Jeśli wybierzesz opcję **Tak, chcę wziąć udział w programie ACEP**, informacje o konfiguracji sprzętowej, najczęściej i najrzadziej używanych funkcjach oraz wszelkich problemach będą automatycznie zbierane z komputera i regularnie wysyłane do firmy Acronis. Wyniki końcowe posłużą do udoskonalenia i zwiększenia funkcjonalności oprogramowania w celu lepszego dostosowania go do potrzeb klientów firmy Acronis.

Firma Acronis nie zbiera żadnych danych osobowych. Aby dowiedzieć się więcej na temat programu ACEP, przeczytaj warunki udziału w witrynie internetowej firmy Acronis lub w graficznym interfejsie użytkownika zainstalowanego programu.

Na początku opcja jest konfigurowana podczas instalacji agenta Acronis Backup & Recovery 10. Ustawienie to można zmienić w dowolnym momencie, korzystając z graficznego interfejsu użytkownika (**Opcje** > **Opcje komputera** > **Program jakości obsługi klienta**). Opcję można również skonfigurować przy użyciu przystawki Zasady grupy (s. 390). Ustawienia określonego za pomocą zasad grupy nie można zmienić w graficznym interfejsie użytkownika programu, chyba że na komputerze zostaną wyłączone zasady grupy.

3.4 Domyślne opcje tworzenia kopii zapasowej i odzyskiwania

3.4.1 Domyślne opcje tworzenia kopii zapasowej

Każdy agent Acronis ma własne domyślne opcje tworzenia kopii zapasowych. Po zainstalowaniu agenta domyślne opcje mają określone wartości, które w dokumentacji są nazywane **wstępnie zdefiniowanymi wartościami**. Podczas tworzenia zadania tworzenia kopii zapasowych można

zastąpić wartość domyślną opcji wartością niestandardową, której program ma użyć w tym konkretnym planie.

Można również dostosować opcję domyślną, zmieniając jej wartość na inną niż wstępnie zdefiniowana. Program będzie domyślnie używał nowej wartości we wszystkich planach tworzenia kopii zapasowych utworzonych na danym komputerze.

Aby wyświetlić i zmienić domyślne opcje tworzenia kopii zapasowych, połącz konsolę z zarządzanym komputerem i z górnego menu wybierz **Opcje > Domyślne opcje tworzenia kopii zapasowej i odzyskiwania > Domyślne opcje tworzenia kopii zapasowej**.

Dostępne opcje tworzenia kopii zapasowych

Zakres dostępnych opcji tworzenia kopii zapasowych zależy od następujących czynników:

- Środowisko działania agenta (Windows, Linux, nośnik startowy)
- Typ danych umieszczanych w kopii zapasowej (dysk, plik)
- Miejsce docelowe kopii zapasowej (lokalizacja sieciowa lub dysk lokalny)
- Schemat tworzenia kopii zapasowych (kopiowanie natychmiastowe lub przy użyciu harmonogramu)

W poniższej tabeli zestawiono dostępność opcji tworzenia kopii zapasowych.

	Agent dla systemu Windows		**Agent dla systemu Linux**		**Nośnik startowy (oparty na systemie Linux lub na środowisku PE)**	
	Kopia zapasowa dysku	**Kopia zapasowa plików**	**Kopia zapasowa dysku**	**Kopia zapasowa plików**	**Kopia zapasowa dysku**	**Kopia zapasowa plików**
Ochrona archiwum (s. 112) (hasło + szyfrowanie)	+	+	+	+	+	+
Wykluczenie plików źródłowych (s. 113)	+	+	+	+	+	+
Polecenia poprzedzające tworzenie kopii zapasowej/następujące po nim (s. 114)	+	+	+	+	Tylko PE	Tylko PE
Polecenia poprzedzające rejestrowanie danych/następujące po nim (s. 116)	+	+	+	+	-	-
Migawka wielowoluminowa (s. 119)	+	+	-	-	-	-
Migawka kopii zapasowej na poziomie pliku (s. 118)	-	+	-	+	-	-
Używanie usługi kopiowania woluminów w tle (s. 119)	+	+	-	-	-	-

Stopień kompresji (s. 120)	+	+	+	+	+	+
Wydajność tworzenia kopii zapasowej:						
Priorytet tworzenia kopii zapasowej (s. 121)	+	+	+	+	-	-
Prędkość zapisu na dysku twardym (s. 121)	Miejsce docelowe: dysk twardy	Miejsce docelowe: dysk twardy	Miejsce docelowe: dysk twardy	Miejsce docelowe: dysk twardy	Miejsce docelowe: dysk twardy	Miejsce docelowe: dysk twardy
Szybkość połączenia sieciowego (s. 121)	Miejsce docelowe: udział sieciowy	Miejsce docelowe: udział sieciowy	Miejsce docelowe: udział sieciowy	Miejsce docelowe: udział sieciowy	Miejsce docelowe: udział sieciowy	Miejsce docelowe: udział sieciowy
Szybka przyrostowa/różnicowa kopia zapasowa (s. 125)	+	-	+	-	+	-
Dzielenie kopii zapasowej (s. 125)	+	+	+	+	+	+
Zabezpieczenia na poziomie plików (s. 126):						
Zachowaj ustawienia zabezpieczeń plików w archiwach	-	+	-	-	-	-
Pliki zaszyfrowane zapisz w archiwach w postaci odszyfrowanej	-	+	-	-	-	-
Komponenty na nośniku	Miejsce docelowe: nośnik wymienny	Miejsce docelowe: nośnik wymienny	Miejsce docelowe: nośnik wymienny	Miejsce docelowe: nośnik wymienny	-	-
Obsługa błędów (s. 127):						
Nie pokazuj komunikatów ani okien dialogowych podczas przetwarzania (tryb dyskretny)	+	+	+	+	+	+
W przypadku wystąpienia błędu spróbuj ponownie	+	+	+	+	+	+
Ignoruj sektory uszkodzone	+	+	+	+	+	+
Dwa miejsca docelowe (s. 128)	Miejsce docelowe: lokalne	Miejsce docelowe: lokalne	Miejsce docelowe: lokalne	Miejsce docelowe: lokalne	-	-
Warunki uruchomienia zadania (s. 129)	+	+	+	+	-	-
Obsługa niepowodzenia zadania (s. 130)	+	+	+	+	-	-
Obsługa taśmy (s. 130)	Miejsce docelowe: skarbiec	Miejsce docelowe: skarbiec	Miejsce docelowe: skarbiec	Miejsce docelowe: skarbiec	Miejsce docelowe: skarbiec	Miejsce docelowe: skarbiec

	zarządzany w bibliotece taśm	zarządzany w bibliotece taśm	zarządzany w bibliotece taśm	zarządzany w bibliotece taśm	zarządzany w bibliotece taśm	zarządzany w bibliotece taśm
Ustawienia dodatkowe (s. 132):						
Zastąp dane na taśmie bez monitowania użytkownika o potwierdzenie	Miejsce docelowe: taśma	Miejsce docelowe: taśma	Miejsce docelowe: taśma	Miejsce docelowe: taśma	Miejsce docelowe: taśma	Miejsce docelowe: taśma
Odmontuj nośnik po utworzeniu kopii zapasowej	Miejsce docelowe: nośnik wymienny	Miejsce docelowe: nośnik wymienny	Miejsce docelowe: nośnik wymienny	Miejsce docelowe: nośnik wymienny	Miejsce docelowe: nośnik wymienny	Miejsce docelowe: nośnik wymienny
W przypadku tworzenia kopii zapasowej na nośnikach wymiennych zapytaj o pierwszy nośnik	Miejsce docelowe: nośnik wymienny	Miejsce docelowe: nośnik wymienny	Miejsce docelowe: nośnik wymienny	Miejsce docelowe: nośnik wymienny	Miejsce docelowe: nośnik wymienny	Miejsce docelowe: nośnik wymienny
Resetuj bit archiwum	-	+	-	-	-	+
Ponownie uruchom komputer po utworzeniu kopii zapasowej	-	-	-	-	+	+
Deduplikuj kopie zapasowe po przetransferowaniu ich do skarbca	Miejsce docelowe: magazyn deduplikacji	Miejsce docelowe: magazyn deduplikacji	Miejsce docelowe: magazyn deduplikacji	Miejsce docelowe: magazyn deduplikacji	Miejsce docelowe: magazyn deduplikacji	Miejsce docelowe: magazyn deduplikacji
Użyj usługi FTP w trybie aktywnym	Miejsce docelowe: serwer FTP	Miejsce docelowe: serwer FTP	Miejsce docelowe: serwer FTP	Miejsce docelowe: serwer FTP	Miejsce docelowe: serwer FTP	Miejsce docelowe: serwer FTP
Razem z kopiami zapasowymi zapisz metadane programowej macierzy RAID i woluminu LVM	-	-	+	-	-	-
Powiadomienia:						
Poczta e-mail (s. 122)	+	+	+	+	-	-
WinPopup (s. 123)	+	+	+	+	-	-
Śledzenie zdarzeń:						
Dziennik zdarzeń systemu Windows (s. 124)	+	+	-	-	-	-
SNMP (s. 124)	+	+	+	+	-	-

Ochrona archiwum

Ta opcja ma zastosowanie w systemach operacyjnych Windows i Linux oraz w przypadku nośników startowych.

Ta opcja jest dostępna zarywno podczas tworzenia kopii zapasowej na poziomie dysku, jak i kopii zapasowej na poziomie plikyw.

Ustawienie wstępne: **Wyłączone**.

Aby zabezpieczyć archiwum przed nieuprawnionym dostępem

1. Zaznacz pole wyboru **Ustaw hasło do archiwum**.
2. W polu **Wprowadź hasło** wpisz hasło.
3. W polu **Potwierdź hasło** wpisz ponownie hasło.
4. Wybierz jedną z następujących opcji:
   - **Nie szyfruj** — archiwum będzie chronione jedynie hasłem.
   - **AES 128** — archiwum zostanie zaszyfrowane przy użyciu algorytmu Advanced Encryption Standard (AES) z kluczem 128-bitowym.
   - **AES 192** — archiwum zostanie zaszyfrowane przy użyciu algorytmu AES z kluczem 192-bitowym.
   - **AES 256** — archiwum zostanie zaszyfrowane przy użyciu algorytmu AES z kluczem 256-bitowym.
5. Kliknij **OK**.

Algorytm kryptograficzny AES działa w trybie wiązania blokyw szyfrogramu (Cipher-Block Chaining — CBC) i korzysta z losowo wygenerowanego klucza o długości zdefiniowanej przez użytkownika: 128, 192 lub 256 bityw. Im większy rozmiar klucza, tym dłużej trwa szyfrowanie archiwum, ale dane są lepiej zabezpieczone.

Klucz szyfrowania jest następnie szyfrowany metodą AES-256, w ktyrej jako klucz służy skryt SHA-256 hasła. Same hasło nie jest przechowywane w żadnym miejscu na dysku ani w pliku kopii zapasowej — do celyw weryfikacji służy skryt hasła. Dzięki tym dwupoziomowym zabezpieczeniom dane kopii zapasowej są chronione przed nieautoryzowanym dostępem, ale odzyskanie utraconego hasła jest niemożliwe.

Wykluczenie plików źródłowych

Ta opcja ma zastosowanie w systemach operacyjnych Windows i Linux oraz w przypadku nośników startowych.

Ta opcja dotyczy kopii zapasowych na poziomie dysków tylko z systemami plików NTFS i FAT oraz kopii zapasowych na poziomie plików we wszystkich obsługiwanych systemach plików.

Opcja określa, które pliki i foldery program ma pominąć w procesie tworzenia kopii zapasowej, a tym samym wykluczyć z listy elementów dodawanych do kopii zapasowej.

Wstępnie zdefiniowaną wartością jest: **Wyklucz pliki spełniające następujące kryteria: *.tmp, *.~, *.bak.**

Aby określić pliki i foldery do wykluczenia:

Skonfiguruj dowolne z następujących parametrów:

- **Wyklucz wszystkie ukryte pliki i foldery**

  Opcja ta działa tylko w systemach plików obsługiwanych przez system Windows. Zaznacz to pole wyboru, aby pominąć pliki i foldery z atrybutem **Ukryty**. Jeśli folder jest **ukryty**, program wykluczy całą jego zawartość, w tym również pliki, które nie mają atrybutu **Ukryty**.
- **Wyklucz wszystkie pliki i foldery systemowe**

  Opcja ta działa tylko w systemach plików obsługiwanych przez system Windows. Zaznacz to pole wyboru, aby pominąć pliki i foldery z atrybutem **Systemowy**. Jeśli folder jest **systemowy**, program wykluczy całą jego zawartość, w tym również pliki, które nie mają atrybutu **Systemowy**.

*Atrybuty plików i folderów można sprawdzić w ich właściwościach lub używając polecenia **attrib**. Więcej informacji można znaleźć w Centrum pomocy i obsługi technicznej w systemie Windows.*

- **Wyklucz pliki spełniające następujące kryteria**

  Zaznacz to pole wyboru, aby pominąć pliki i foldery, których nazwy pasują do podanych na liście kryteriów zwanych maskami plików. Aby utworzyć listę masek plików, użyj przycisków **Dodaj**, **Edytuj**, **Usuń** i **Usuń wszystko**.

  W masce plików można użyć jednego lub kilku symboli wieloznacznych * i ?:

  Gwiazdka (*) zastępuje dowolną liczbę znaków w nazwie pliku (w tym również zero). Na przykład maska Dok*.txt zwraca pliki takie jak Dok.txt i Dokument.txt.

  Znak zapytania (?) zastępuje dokładnie jeden znak w nazwie pliku. Na przykład maska Dok?.txt zwraca pliki takie jak Dok1.txt i Doku.txt, ale nie zwraca plików Dok.txt ani Dok11.txt.

Aby wykluczyć folder określony przez ścieżkę zawierającą literę dysku, dodaj ukośnik odwrotny (\) do nazwy folderu w kryterium, np.: C:\Finanse\

Przykłady wykluczeń

Kryterium	Przykład	Opis
Windows i Linux		
Według nazwy	F.log F	Wyklucza wszystkie pliki o nazwie „F.log”. Wyklucza wszystkie foldery o nazwie „F”.
Według maski (*)	*.log F*	Wyklucza wszystkie pliki z rozszerzeniem .log. Wyklucza wszystkie pliki i foldery, których nazwa rozpoczyna się od litery „F” (np. foldery F, F1 i pliki F.log, F1.log).
Według maski (?)	F???.log	Wyklucza wszystkie pliki z rozszerzeniem .log, których nazwy składają się z czterech znaków i zaczynają od litery „F”.
Windows		
Według ścieżki pliku	C:\Finanse\F.log	Wyklucza plik „F.log” znajdujący się w folderze C:\Finanse.
Według ścieżki folderu	C:\Finanse\F\	Wyklucza folder C:\Finanse\F (należy określić pełną ścieżkę, rozpoczynającą się od litery dysku).
Linux		
Według ścieżki pliku	/home/user/Finanse/F.log	Wyklucza plik „F.log” znajdujący się w folderze /home/user/Finanse.
Według ścieżki folderu	/home/user/Finanse/	Wyklucza folder /home/user/Finanse.

Powyższe ustawienia nie dotyczą plików lub folderów jawnie wybranych do utworzenia kopii zapasowej. Przyjmijmy na przykład, że użytkownik wybrał folder MójFolder oraz plik MójPlik.tmp znajdujący się poza tym folderem, oraz określił opcję pomijania wszystkich plików .tmp. Wówczas wszystkie pliki .tmp w folderze MójFolder zostaną pominięte w procesie tworzenia kopii zapasowej, ale program nie pominie pliku MójPlik.tmp.

Polecenia poprzedzające/następujące

Ta opcja ma zastosowanie w systemach operacyjnych Windows i Linux oraz w przypadku nośników startowych opartych na środowisku PE.

Ta opcja umożliwia określenie poleceń wykonywanych automatycznie przed utworzeniem kopii zapasowej i po jego zakończeniu.

Poniższy schemat przedstawia czas wykonania poleceń poprzedzających/następujących.

Polecenie poprzedzające utworzenie kopii zapasowej	Utworzenie kopii zapasowej	Polecenie następujące po utworzeniu kopii zapasowej

Przykłady zastosowania poleceń poprzedzających/następujących:

- usuwanie tymczasowych plików z dysku przed rozpoczęciem tworzenia kopii zapasowej.
- konfigurowanie produktów antywirusowych innych producentów w celu ich uruchomienia przed każdym rozpoczęciem tworzenia kopii zapasowej.
- kopiowanie i archiwizowanie w innej lokalizacji po utworzeniu kopii zapasowej.

Program nie obsługuje poleceń interaktywnych wymagających działania użytkownika (na przykład „pause").

Aby określić polecenia poprzedzające/następujące

1. Włącz wykonywanie poleceń poprzedzających/następujących, zaznaczając następujące opcje:
   - **Wykonaj przed utworzeniem kopii zapasowej**
   - **Wykonaj po utworzeniu kopii zapasowej**
2. Wykonaj jedną z następujących czynności:
   - Kliknij **Edytuj**, aby określić nowe polecenie lub plik wsadowy.
   - Wybierz istniejące polecenie lub plik wsadowy z listy rozwijanej.
3. Kliknij **OK**.

Polecenie poprzedzające utworzenie kopii zapasowej

Aby określić polecenie/plik wsadowy do wykonania przed rozpoczęciem procesu tworzenia kopii zapasowej

1. W polu **Polecenie** wpisz polecenie lub wskaż plik wsadowy. Program nie obsługuje poleceń interaktywnych, to znaczy poleceń wymagających działania użytkownika (na przykład „pause".)
2. W polu **Katalog roboczy** określ ścieżkę do katalogu, w którym zostanie wykonane polecenie lub plik wsadowy.
3. W polu **Argumenty** określ argumenty wykonywania polecenia, jeśli są wymagane.
4. W zależności od wyniku, który chcesz uzyskać, wybierz odpowiednie opcje opisane w poniższej tabeli.
5. Kliknij **Testuj polecenie**, aby sprawdzić, czy polecenie jest prawidłowe.

Pole wyboru	**Wybór**			
Zakończ zadanie niepowodzeniem, jeśli wykonanie polecenia się nie powiedzie	Wybrane	Niewybrane	Wybrane	Niewybrane
Nie twórz kopii zapasowej przed zakończeniem wykonywania polecenia	Wybrane	Wybrane	Niewy-brane	Niewybrane

	Wynik			
	Ustawienie wstępne Utwórz kopię zapasową tylko po pomyślnym wykonaniu polecenia. Zakończ zadanie niepowodzeniem, jeśli wykonanie polecenia się nie powiedzie.	Utwórz kopię zapasową po wykonaniu polecenia, niezależnie od tego, czy zakończyło się powodzeniem, czy niepowodzeniem.	N/D	Utwórz kopię zapasową równolegle z wykonywaniem polecenia i niezależnie od wyniku jego wykonania.

Polecenie następujące po utworzeniu kopii zapasowej

Aby określić polecenie/plik wykonywalny, które mają zostać wykonane po zakończeniu tworzenia kopii zapasowej

1. W polu **Polecenie** wpisz polecenie lub wskaż plik wsadowy.
2. W polu **Katalog roboczy** określ ścieżkę do katalogu, w którym zostanie wykonane polecenie lub plik wsadowy.
3. W polu **Argumenty** określ argumenty wykonywania polecenia, jeśli są wymagane.
4. Jeśli pomyślne wykonanie polecenia ma znaczenie krytyczne dla strategii tworzenia kopii zapasowych, należy zaznaczyć pole wyboru **Zakończ zadanie niepowodzeniem, jeśli wykonanie polecenia się nie powiedzie**. W przypadku niepowodzenia wykonania polecenia program, jeśli to będzie możliwe, usunie wynikowy plik TIB i pliki tymczasowe i zadanie zakończy się niepowodzeniem.

   Jeśli to pole wyboru nie jest zaznaczone, wynik wykonania polecenia nie wpływa na powodzenie lub niepowodzenie wykonania zadania. Wynik wykonania polecenia można sprawdzić w dzienniku lub na liście Błędy i ostrzeżenia wyświetlonej na **Pulpicie nawigacyjnym**.
5. Kliknij **Testuj polecenie**, aby sprawdzić, czy polecenie jest prawidłowe.

Polecenia poprzedzające rejestrowanie danych/następujące po nim

Ta opcja ma zastosowanie zarówno w systemach operacyjnych Windows, jak i Linux.

Ta opcja umożliwia określenie poleceń wykonywanych automatycznie przed zarejestrowaniem danych i po jego zakończeniu (czyli wykonaniu migawki danych). Migawka jest wykonywana przez program Acronis Backup & Recovery 10 na początku procedury tworzenia kopii zapasowej.

Poniższy schemat przedstawia czas wykonania poleceń poprzedzających i następujących po rejestrowaniu danych.

	<---------- **Kopia zapasowa** ---------->			
Polecenie poprzedzające utworzenie kopii zapasowej	Polecenie poprzedzające rejestrowanie danych	Rejestrowanie danych	Polecenie następujące po zarejestrowaniu danych	Polecenie następujące po utworzeniu kopii zapasowej

Jeśli opcja Usługa kopiowania woluminów w tle (s. 119) jest włączona, wykonywanie poleceń i czynności usługi Microsoft VSS odbędzie się w następującej kolejności:

Polecenia „Przed zarejestrowaniem danych” -> Wstrzymanie VSS -> Rejestrowanie danych -> Wznowienie VSS -> Polecenia „Po zarejestrowaniu danych”.

Przy użyciu poleceń wykonywanych przed rejestrowaniem danych lub po jego zakończeniu można zawiesić lub wznowić działanie bazy danych lub aplikacji, która nie jest kompatybilna z usługą VSS. W

przeciwieństwie do poleceń poprzedzających/następujących (s. 114) polecenia poprzedzające rejestrowanie danych i następujące po nim są wykonywane przed procesem rejestrowania danych i po jego zakończeniu. Trwa to kilka sekund. Tworzenie kopii zapasowej może natomiast zająć dużo więcej czasu, w zależności od ilości danych. Dlatego czas przestoju bazy danych lub aplikacji jest minimalny.

Aby określić polecenia poprzedzające rejestrowanie danych/następujące po nim

1. Włącz wykonywanie poleceń poprzedzających rejestrowanie danych/następujących po nim, zaznaczając następujące opcje:
   - **Wykonaj przed zarejestrowaniem danych**
   - **Wykonaj po zarejestrowaniu danych**
2. Wykonaj jedną z następujących czynności:
   - Kliknij **Edytuj**, aby określić nowe polecenie lub plik wsadowy.
   - Wybierz istniejące polecenie lub plik wsadowy z listy rozwijanej.
3. Kliknij **OK**.

Polecenie poprzedzające rejestrowanie danych

Aby określić polecenie/plik wsadowy do wykonania przed rozpoczęciem procesu rejestrowania danych

1. W polu **Polecenie** wpisz polecenie lub wskaż plik wsadowy. Program nie obsługuje poleceń interaktywnych, to znaczy poleceń wymagających działania użytkownika (na przykład „pause”.)
2. W polu **Katalog roboczy** określ ścieżkę do katalogu, w którym zostanie wykonane polecenie lub plik wsadowy.
3. W polu **Argumenty** określ argumenty wykonywania polecenia, jeśli są wymagane.
4. W zależności od wyniku, który chcesz uzyskać, wybierz odpowiednie opcje opisane w poniższej tabeli.
5. Kliknij **Testuj polecenie**, aby sprawdzić, czy polecenie jest prawidłowe.

Pole wyboru	**Wybór**			
Zakończ niepowodzeniem tworzenie kopii zapasowej, jeśli wykonanie polecenia się nie powiedzie	Wybrane	Niewybrane	Wybrane	Niewybrane
Nie rejestruj danych przed zakończeniem wykonywania polecenia	Wybrane	Wybrane	Niewy-brane	Niewybrane
Wynik				
	Ustawienie wstępne Zarejestruj dane tylko po pomyślnym wykonaniu polecenia. Zakończ zadanie niepowodzeniem, jeśli wykonanie polecenia się nie powiedzie.	Zarejestruj dane po wykonaniu polecenia, niezależnie od tego, czy zakończyło się powodzeniem, czy niepowodzeniem.	N/D	Zarejestruj dane równolegle z wykonywaniem polecenia i niezależnie od wyniku jego wykonania.

Polecenie następujące po zarejestrowaniu danych

Aby określić polecenie/plik wsadowy do wykonania po zarejestrowaniu danych

1. W polu **Polecenie** wpisz polecenie lub wskaż plik wsadowy. Program nie obsługuje poleceń interaktywnych, to znaczy poleceń wymagających działania użytkownika (na przykład „pause”.)
2. W polu **Katalog roboczy** określ ścieżkę do katalogu, w którym zostanie wykonane polecenie lub plik wsadowy.
3. W polu **Argumenty** określ argumenty wykonywania polecenia, jeśli są wymagane.
4. W zależności od wyniku, który chcesz uzyskać, wybierz odpowiednie opcje opisane w poniższej tabeli.
5. Kliknij **Testuj polecenie**, aby sprawdzić, czy polecenie jest prawidłowe.

Pole wyboru	**Wybór**			
Zakończ zadanie niepowodzeniem, jeśli wykonanie polecenia się nie powiedzie	Wybrane	Niewybrane	Wybrane	Niewybrane
Nie twórz kopii zapasowej przed zakończeniem wykonywania polecenia	Wybrane	Wybrane	Niewy-brane	Niewybrane
Wynik				
	Ustawienie wstępne Kontynuuj tworzenie kopii zapasowej tylko po pomyślnym wykonaniu polecenia. Usuń plik TIB i pliki tymczasowe i zakończ zadanie niepowodzeniem w przypadku, gdy wykonanie polecenia się nie powiedzie.	Kontynuuj tworzenie kopii zapasowej po wykonaniu polecenia, niezależnie od tego, czy zakończyło się powodzeniem, czy niepowodzeniem.	N/D	Kontynuuj tworzenie kopii zapasowej równolegle z wykonywaniem polecenia i niezależnie od wyniku jego wykonania.

Migawka kopii zapasowej na poziomie pliku

Ta opcja ma zastosowanie tylko w przypadku kopii zapasowych na poziomie pliku. Ta opcja ma zastosowanie w systemach operacyjnych Windows i Linux.

Ta opcja określa, czy kopia zapasowa ma być tworzona kolejno dla poszczególnych plików, czy też ma zostać utworzona migawka.

Uwaga: *Pliki zapisane w udostępnionych zasobach sieciowych są zawsze dodawane do kopii zapasowej kolejno.*

Ustawienie wstępne: **Utwórz migawkę, jeśli to możliwe.**

Wybierz jedną z następujących opcji:

- **Zawsze twórz migawkę**

  Migawka umożliwia utworzenie kopii zapasowej wszystkich plików, w tym plików otwartych do wyłącznego dostępu. Kopia zapasowa plików zostanie utworzona w tym samym momencie. To ustawienie należy wybrać tylko wówczas, gdy czynniki te mają krytyczne znaczenie, tzn.

utworzenie kopii zapasowej bez tworzenia migawki nie ma sensu. Aby użyć migawki, plan utworzenia kopii zapasowej musi być uruchomiony z konta z uprawnieniami administratora lub operatora kopii zapasowej. Jeśli nie można utworzyć migawki, utworzenie kopii zapasowej zakończy się niepowodzeniem.

- **Utwórz migawkę, jeśli to możliwe**

  Jeśli nie można wykonać migawki, należy utworzyć bezpośrednią kopię zapasową plików.

- **Nie twórz migawki**

  Zawsze wykonuj bezpośrednią kopię zapasową plików. Uprawnienia administratora lub operatora kopii zapasowej nie są wymagane. Próba utworzenia kopii zapasowej plików otwartych do wyłącznego dostępu zakończy się błędem odczytu. Pliki w kopii zapasowej mogą być utworzone w różnych chwilach.

Migawka wielowoluminowa

Ta opcja ma zastosowanie tylko w systemach operacyjnych Windows..

Ta opcja dotyczy kopii zapasowej na poziomie dysku. Ma również zastosowanie w przypadku kopii zapasowej na poziomie pliku, gdy jest ona wykonywana przez utworzenie migawki. (Opcja Migawka kopii zapasowej na poziomie pliku (s. 118) określa, czy podczas tworzenia kopii zapasowej na poziomie pliku zostanie utworzona migawka).

Opcja określa, czy migawki kilku woluminów mają być tworzone jednocześnie czy kolejno.

Ustawienie wstępne: **Włączone**.

Gdy opcja ta ma wartość **Włączone**, migawki wszystkich woluminów są tworzone jednocześnie. Opcji tej należy używać w celu utworzenia w jednej chwili kopii zapasowej danych na kilku woluminach, na przykład bazy danych Oracle.

Gdy opcja ta ma wartość **Wyłączone**, migawki woluminów będą tworzone kolejno. W efekcie, jeśli dane są rozłożone na kilku woluminach, kopia zapasowa może zawierać pliki utworzone w różnych chwilach.

Usługa kopiowania woluminów w tle

Ta opcja ma zastosowanie tylko w systemach operacyjnych Windows..

Ta opcja określa, czy Usługa kopiowania woluminów w tle udostępniana przez firmę Microsoft (VSS) ma powiadamiać aplikacje obsługujące technologię VSS o rozpoczęciu tworzenia kopii zapasowej.

Ustawienie wstępne: **Wyłącz obsługę Usługi kopiowania woluminów w tle**

Usługa kopiowania woluminów w tle udostępniana przez firmę Microsoft (VSS) zapewnia infrastrukturę do tworzenia kopii zapasowych danych w działających systemach, zapewniając koordynację pomiędzy aplikacjami aktualizującymi dane na dyskach a aplikacjami do tworzenia kopii zapasowych. Przykładami serwerów baz danych obsługujących technologię VSS są Microsoft Exchange i Microsoft SQL Server.

Opcję **Usługa kopiowania woluminów w tle** należy włączyć, gdy dowolna baza danych lub aplikacja jest zgodna z usługą VSS. Usługa VSS powiadomi aplikację obsługującą tę technologię o rozpoczęciu tworzenia kopii zapasowej. Umożliwia to zapewnienie spójnego stanu wszystkich danych używanych przez aplikacje, a zwłaszcza dokończenie wszystkich transakcji baz danych w momencie utworzenia migawki przez program Acronis Backup & Recovery 10. Spójność danych zapewnia z kolei możliwość odzyskania aplikacji w prawidłowym stanie i umożliwia rozpoczęcie jej używania natychmiast po odzyskaniu.

Migawki utworzone przy użyciu usługi VSS nie są używane.

Jeśli baza danych nie jest zgodna z usługą VSS, należy użyć opcji Polecenia poprzedzające rejestrowanie danych/następujące po nim (s. 116), aby określić polecenia, które powinny zostać wykonane przed utworzeniem migawki i po nim w celu zapewnienia spójności danych dodawanych do kopii zapasowej. Można na przykład określić polecenia poprzedzające rejestrowanie danych, które spowodują wstrzymanie działania bazy danych i wyczyszczenie pamięci podręcznej w celu dokończenia wszystkich transakcji, a także polecenia po rejestrowaniu danych, które spowodują wznowienie działania bazy danych po utworzeniu migawki.

Programy zapisujące usługi kopiowania woluminów w tle

Przed utworzeniem kopii zapasowej danych aplikacji obsługujących usługę VSS należy upewnić się, że są włączone programy zapisujące usługi kopiowania woluminów w tle, sprawdzając listę programów zapisujących w systemie operacyjnym. Aby wyświetlić tę listę, należy wykonać następujące polecenie:

```
vssadmin list writers
```

Uwaga: *W systemie Microsoft Windows Small Business Server 2003 program zapisujący dla Microsoft Exchange Server 2003 jest domyślnie wyłączony. Instrukcje na temat jego włączenia można znaleźć w odpowiednim artykule pomocy i wsparcia firmy Microsoft http://support.microsoft.com/kb/838183/pl.*

Stopień kompresji

Ta opcja jest przeznaczona dla systemów operacyjnych Windows i Linux oraz nośników startowych.

Określa ona poziom kompresji danych w tworzonej kopii zapasowej.

Ustawienie wstępne: **Normalna**.

Optymalny poziom kompresji danych zależy od typu danych dodawanych do kopii zapasowej. Na przykład nawet maksymalny poziom kompresji nie zmniejszy znacząco rozmiaru archiwum, jeśli zawiera ono głównie skompresowane pliki, takie jak .jpg, .pdf lub .mp3. Jednak pliki w formatach takich jak .doc lub .xls będą dobrze skompresowane.

Aby określić poziom kompresji

Wybierz jedną z następujących opcji:

- **Brak** — dane zostaną skopiowane bez kompresji. Otrzymana kopia zapasowa będzie miała maksymalny rozmiar.
- **Normalny** — ustawienie zalecane w większości przypadków.
- **Wysoka** — otrzymana kopia zapasowa będzie zazwyczaj mniejsza niż w przypadku użycia ustawienia **Normalna**.
- **Maksymalna** — dane zostaną skompresowane w maksymalnym stopniu. Czas tworzenia kopii zapasowej będzie najdłuższy. Maksymalny poziom kompresji należy wybierać w przypadku tworzenia kopii zapasowej na nośnikach wymiennych w celu zmniejszenia liczby wymaganych nośników.

Wydajność tworzenia kopii zapasowej

Ta grupa opcji umożliwia określenie ilości zasobów sieciowych i systemowych przydzielonych do procesu tworzenia kopii zapasowej.

Opcje wydajności tworzenia kopii zapasowej mogą mieć większy lub mniejszy wpływ na szybkość tworzenia kopii zapasowej. Zależy to od ogólnej konfiguracji systemu i fizycznej charakterystyki urządzeń biorących udział w procesie tworzenia kopii zapasowej.

Priorytet tworzenia kopii zapasowej

Ta opcja jest uwzględniana w systemach operacyjnych Windows i Linux.

Priorytet procesu uruchomionego w systemie określa ilość zasobów procesora i systemu przydzielonych do tego procesu. Zmniejszenie priorytetu procesu tworzenia kopii zapasowej spowoduje zwolnienie większej ilości zasobów dla innych aplikacji. Zwiększenie priorytetu procesu tworzenia kopii zapasowej może go przyspieszyć dzięki przydzieleniu większej ilości zasobów, np. procesora, dla aplikacji do tworzenia kopii zapasowej. Końcowy efekt zależy jednak od ogólnego obciążenia procesora i innych czynników, takich jak prędkość zapisu/odczytu dysków i obciążenie sieci.

Ustawienie wstępne: **Niski**.

Aby określić priorytet procesu tworzenia kopii zapasowej

Wybierz jedną z następujących opcji:

- **Niski** — minimalizuje ilość zasobów wykorzystywanych przez proces tworzenia kopii zapasowej, pozostawiając więcej zasobów dla innych procesów uruchomionych na komputerze
- **Normalny** — proces tworzenia kopii zapasowej działa z normalną prędkością, wykorzystując podobną ilość zasobów jak inne procesy
- **Wysoki** — proces tworzenia kopii zapasowej działa z maksymalną prędkością, wykorzystując zasoby, które były używane przez inne procesy

Prędkość zapisu na dysku twardym

Ta opcja jest dostępna w przypadku systemów operacyjnych Windows i Linux oraz nośnika startowego.

Opcja jest dostępna, gdy jako miejsce docelowe kopii zapasowej został wybrany wewnętrzny dysk twardy komputera, którego kopia zapasowa jest tworzona.

Tworzenie kopii zapasowej na stałym dysku twardym (na przykład w strefie Acronis Secure Zone) może spowolnić działanie systemu operacyjnego i aplikacji z powodu dużej ilości danych zapisywanych na dysku. Wykorzystanie dysku twardego w procesie tworzenia kopii zapasowej można ograniczyć do odpowiedniego poziomu.

Ustawienie wstępne: **Maksymalna**.

Aby ustawić żądaną prędkość zapisu na dysku twardym w procesie tworzenia kopii zapasowej

Wykonaj jedną z następujących czynności:

- Kliknij **Prędkość zapisu określona jako wartość procentowa prędkości maksymalnej na docelowym dysku twardym** i przeciągnij suwak lub wybierz wartość procentową w polu.
- Kliknij **Prędkość zapisu wyrażona w kilobajtach na sekundę** i wprowadź prędkość zapisu w kilobajtach na sekundę.

Szybkość połączenia sieciowego

Ta opcja jest przeznaczona dla systemów operacyjnych Windows i Linux oraz nośników startowych.

Ta opcja jest dostępna po wybraniu lokalizacji sieciowej (udziału sieciowego, zarządzanego skarbca lub serwera FTP/SFTP) jako miejsca docelowego dla kopii zapasowej.

Opcja określa wartość przepustowości łącza sieciowego przeznaczoną do przesyłania kopiowanych danych.

Domyślnie jest ustawiona maksymalna prędkość, tzn. oprogramowanie używa pełnej przepustowości podczas przesyłania danych kopii zapasowej. Ta opcja umożliwia zarezerwowanie pewnej przepustowości dla innych aplikacji sieciowych.

Ustawienie wstępne: **Maksymalna**.

Aby ustawić prędkość połączenia sieciowego dla tworzenia kopii zapasowej

Wykonaj jedną z następujących czynności:

- Kliknij **Prędkość transferu określona jako wartość procentowa szacowanej prędkości maksymalnej połączenia sieciowego**, i przeciągnij suwak lub wpisz wartość procentową w polu.
- Kliknij **Prędkość transferu wyrażona w kilobajtach na sekundę**, a następnie wprowadź limit przepustowości dla przesyłania danych kopii zapasowej w kilobajtach na sekundę.

Powiadomienia

Program Acronis Backup & Recovery 10 umożliwia powiadamianie użytkowników o utworzeniu kopii zapasowej przy użyciu poczty e-mail lub usługi komunikacyjnej.

Poczta e-mail

Ta opcja jest uwzględniana w systemach operacyjnych Windows i Linux.

Jest ona niedostępna podczas pracy z nośnikiem startowym.

Ta opcja umożliwia odbieranie pocztą e-mail pełnego dziennika zadania oraz powiadomień o pomyślnym zakończeniu zadania utworzenia kopii zapasowej, niepowodzeniu wykonania zadania lub konieczności podjęcia działania.

Ustawienie wstępne: **Wyłączone**.

Aby skonfigurować powiadamianie pocztą e-mail

1. Zaznacz pole wyboru **Wysyłaj powiadomienia pocztą e-mail**, aby włączyć powiadamianie.
2. W polu **Adresy e-mail** wpisz adresy e-mail, na które chcesz wysłać powiadomienia. Możesz wpisać kilka adresów rozdzielonych średnikami.
3. W sekcji **Wysyłaj powiadomienia** zaznacz odpowiednie pola wyboru
   - **Po pomyślnym utworzeniu kopii zapasowej** — aby wysłać powiadomienia po pomyślnym utworzeniu kopii zapasowej
   - **Gdy utworzenie kopii zapasowej się nie powiedzie** — aby wysłać powiadomienia, gdy utworzenie kopii zapasowej nie powiedzie się

   Pole wyboru **Gdy jest konieczne działanie użytkownika** jest zawsze zaznaczone.
4. Aby wiadomość e-mail zawierała wpisy dziennika związane z tworzeniem kopii zapasowej, zaznacz pole wyboru **Dodaj do powiadomienia pełny dziennik**.
5. Kliknij **Dodatkowe parametry poczty e-mail**, aby skonfigurować przedstawione poniżej parametry poczty e-mail, a następnie kliknij **OK**:
   - **Od** — wpisz adres e-mail użytkownika, który będzie nadawcą wiadomości. Jeśli to pole pozostanie puste, w polu nadawcy program wpisze adresata wiadomości.
   - **Użyj szyfrowania** — umożliwia włączenie szyfrowanego połączenia z serwerem poczty. Można wybrać szyfrowanie SSL lub TLS.

- Niektórzy dostawcy usług internetowych wymagają uwierzytelniania na serwerze poczty przychodzącej przed umożliwieniem wysłania wiadomości. Jeśli tak jest, zaznacz pole wyboru **Zaloguj się na serwerze poczty przychodzącej**, aby umożliwić używanie serwera POP i skonfigurować jego ustawienia:
  - **Serwer poczty przychodzącej (POP)** — wprowadź nazwę serwera POP.
  - **Port** — ustaw port serwera POP. Domyślnie jest ustawiony port 110.
  - **Nazwa użytkownika** — wprowadź nazwę użytkownika.
  - **Hasło** — wprowadź hasło.
- Zaznacz pole wyboru **Użyj określonego serwera poczty wychodzącej**, aby umożliwić używanie serwera SMTP i skonfigurować jego ustawienia:
  - **Serwer poczty wychodzącej (SMTP)** — wprowadź nazwę serwera SMTP.
  - **Port** — ustaw port serwera SMTP. Domyślnie jest ustawiony port 25.
  - **Nazwa użytkownika** — wprowadź nazwę użytkownika.
  - **Hasło** — wprowadź hasło.

6. Kliknij **Wyślij próbną wiadomość e-mail**, aby sprawdzić, czy ustawienia są poprawne.

Usługa Messenger (WinPopup)

Ta opcja działa w systemach operacyjnych Windows i Linux na komputerach wysyłających i tylko w systemie Windows na komputerach odbierających.

Jest ona niedostępna podczas pracy z nośnikiem startowym.

Opcja umożliwia odbieranie powiadomień WinPopup informujących o pomyślnym wykonaniu zadania, niepowodzeniu lub konieczności podjęcia działania.

Ustawienie wstępne: **Wyłączone**.
Przed skonfigurowaniem powiadomień WinPopup należy dopilnować, aby usługa Messenger była włączona na obu komputerach: wykonującym zadanie i odbierającym wiadomości.

Usługa Messenger nie jest domyślnie uruchamiana w systemach z grupy Microsoft Windows Server 2003. Zmień tryb uruchamiania usługi na Automatyczny i uruchom usługę.

Aby skonfigurować powiadomienia WinPopup:

1. Zaznacz pole wyboru **Wysyłaj powiadomienia WinPopup**.
2. W polu **Nazwa komputera** wprowadź nazwę komputera, do którego chcesz przesyłać powiadomienia. Używanie kilku nazw nie jest obsługiwane.

W sekcji **Wysyłaj powiadomienia** zaznacz odpowiednie pola wyboru

- **Po pomyślnym utworzeniu kopii zapasowej** — powiadomienie jest wysyłane po pomyślnym utworzeniu kopii zapasowej
- **Gdy utworzenie kopii zapasowej się nie powiedzie** — powiadomienie jest wysyłane, gdy utworzenie kopii zapasowej się nie powiedzie

Pole wyboru **Gdy jest konieczne działanie użytkownika** — powiadomienie jest wysyłane w czasie trwania operacji, gdy wymagane jest podjęcie działania przez użytkownika. To pole jest zawsze wybrane.

Kliknij **Wyślij próbny komunikat WinPopup**, aby sprawdzić, czy ustawienia są poprawne.

Śledzenie zdarzeń

Zdarzenia w dzienniku dotyczące wszystkich operacji tworzenia kopii zapasowej wykonanych na komputerze zarządzanym można zduplikować w dzienniku zdarzeń aplikacji systemu Windows lub wysłać do określonych menedżerów SNMP.

Dziennik zdarzeń systemu Windows

Ta opcja jest uwzględniana tylko w systemach operacyjnych Windows.

Jest ona niedostępna podczas pracy z nośnikiem startowym.

Ta opcja określa, czy agenty działające na komputerze zarządzanym muszą rejestrować zdarzenia operacji tworzenia kopii zapasowych w dzienniku zdarzeń aplikacji systemu Windows (aby wyświetlić ten dziennik, uruchom program **eventvwr.exe** lub wybierz kolejno: **Panel sterowania > Narzędzia administracyjne > Podgląd zdarzeń**). Zarejestrowane zdarzenia można filtrować.

Ustawienie wstępne: **Użyj ustawień określonych w obszarze Komputer.**

Aby określić, czy zdarzenia operacji tworzenia kopii zapasowych mają być rejestrowane w dzienniku zdarzeń aplikacji systemu Windows:

Wybierz jedną z następujących opcji:

- **Użyj ustawień określonych w obszarze Komputer** — aby użyć ustawienia określonego dla komputera. Aby uzyskać więcej informacji, zapoznaj się z sekcją Opcje komputera (s. 105).
- **Rejestruj zdarzenia następujących typów** — aby rejestrować zdarzenia operacji tworzenia kopii zapasowych w dzienniku zdarzeń aplikacji. Należy określić typy rejestrowanych zdarzeń:
  - **Wszystkie zdarzenia** — rejestrowane są wszystkie zdarzenia (informacje, ostrzeżenia i błędy)
  - **Błędy i ostrzeżenia**
  - **Tylko błędy**
- **Nie rejestruj** — aby wyłączyć rejestrowanie zdarzeń operacji tworzenia kopii zapasowych w dzienniku zdarzeń aplikacji.

Powiadomienia SNMP

Ta opcja jest uwzględniana w systemach operacyjnych Windows i Linux.

Jest ona niedostępna podczas pracy z nośnikiem startowym.

Ta opcja określa, czy agenty działające na komputerze zarządzanym muszą wysyłać zdarzenia operacji tworzenia kopii zapasowych z dziennika do określonych menedżerów Simple Network Management Protocol (SNMP). Można wybrać typy wysyłanych zdarzeń.

Aby uzyskać szczegółowe informacje na temat programu Acronis Backup & Recovery 10, zobacz „Obsługa SNMP (s. 59)”.

Ustawienie wstępne: **Użyj ustawień określonych w obszarze Komputer.**

Aby wybrać, czy zdarzenia operacji tworzenia kopii zapasowych mają być wysyłane do menedżerów SNMP:

Wybierz jedną z następujących opcji:

- **Użyj ustawień określonych w obszarze Komputer** — aby użyć ustawienia określonego dla komputera. Aby uzyskać więcej informacji, zapoznaj się z sekcją Opcje komputera (s. 105).

- **Wyślij osobne powiadomienie SNMP dla każdego zdarzenia tworzenia kopii zapasowej** — aby wysyłać informacje o zdarzeniach operacji tworzenia kopii zapasowych do określonych menedżerów SNMP.
  - **Typy wysyłanych zdarzeń** — wybierz typy wysyłanych zdarzeń: **Wszystkie zdarzenia**, **Błędy i ostrzeżenia** lub **Tylko błędy**.
  - **Nazwa/adres IP serwera** — wpisz nazwę lub adres IP hosta, na którym jest uruchomiona aplikacja do zarządzania SNMP, do której chcesz przesyłać komunikaty.
  - **Społeczność** — wpisz nazwę społeczności SNMP, do której należy host z aplikacją do zarządzania SNMP oraz komputer wysyłający. Typowe ustawienie to „publiczna”.

  Kliknij **Wyślij wiadomość próbną**, aby sprawdzić, czy ustawienia są poprawne.
- **Nie wysyłaj powiadomień SNMP** — aby wyłączyć wysłanie zdarzeń z dziennika dotyczących operacji tworzenia kopii zapasowych do menedżerów SNMP.

Szybka przyrostowa/różnicowa kopia zapasowa

Ta opcja jest przeznaczona dla systemów operacyjnych Windows i Linux oraz nośników startowych.

Ta opcja jest uwzględniana podczas tworzenia przyrostowych i różnicowych kopii zapasowych na poziomie dysku.

Określa ona, czy zmiana w pliku jest określana na podstawie jego rozmiaru i daty utworzenia, czy na podstawie porównania zawartości z plikiem zapisanym w archiwum.

Ustawienie wstępne: **Włączone**.

Przyrostowe i różnicowe kopie zapasowe umożliwiają zapisanie jedynie zmienionych danych. Aby przyspieszyć proces tworzenia kopii zapasowej, program określa, czy dany plik uległ modyfikacji na podstawie jego rozmiaru i daty oraz godziny zapisania. Wyłączenie tej funkcji spowoduje, że program będzie porównywał całą zawartość plików z plikami zapisanymi w archiwum.

Dzielenie kopii zapasowej

Ta opcja jest przeznaczona dla systemów operacyjnych Windows i Linux oraz nośników startowych.

Ta opcja umożliwia zdefiniowanie sposobu dzielenia kopii zapasowej.

Ustawienie wstępne: **Automatycznie.**

Dostępne są następujące ustawienia.

Automatycznie

Przy tym ustawieniu program Acronis Backup & Recovery 10 będzie działał w następujący sposób.

- **Podczas tworzenia kopii zapasowej na dysku twardym:**

  Jeżeli system plików dysku docelowego dopuszcza szacowany rozmiar pliku, zostanie utworzony jeden plik kopii zapasowej.

  Jeżeli system plików dysku docelowego nie dopuszcza szacowanego rozmiaru pliku, kopia zapasowa zostanie automatycznie podzielona na kilka plików. Taka sytuacja może wystąpić, jeżeli kopia zapasowa zostanie umieszczona na dysku z systemem plików FAT16 lub FAT32, które posiadają limit rozmiaru pliku 4 GB.

  Jeżeli podczas tworzenia kopii zapasowej na dysku docelowym skończy się wolne miejsce, zadanie przejdzie w stan **Wymagające działania**. Można wówczas zwolnić dodatkowe miejsce na dysku i ponowić operację. W takim przypadku kopia zapasowa zostanie podzielona na części utworzone przed ponowieniem operacji i po nim.

- **Podczas tworzenia kopii zapasowej na nośniku wymiennym** (płyta CD, DVD lub urządzenie taśmowe dołączone lokalnie do komputera zarządzanego):

  Zadanie przejdzie w stan **Wymagające działania** i kiedy nośnik będzie pełny, użytkownik zostanie poproszony o kolejny.

Stały rozmiar

Wprowadź pożądany rozmiar pliku lub wybierz go z listy rozwijanej. Nastąpi podział kopii zapasowej na wiele plików o określonym rozmiarze. Ta funkcja przydaje się podczas tworzenia kopii zapasowej nagrywanej następnie na wielu płytach CD lub DVD. Można również podzielić kopię zapasową przeznaczoną na serwer FTP, ponieważ odzyskiwanie danych bezpośrednio z serwera FTP wymaga podzielenia kopii zapasowej na pliki o rozmiarze nie większym niż 2 GB.

Zabezpieczenia na poziomie plików

Te opcje są uwzględniane tylko w przypadku kopii zapasowej na poziomie plików w systemach operacyjnych Windows.

Pliki zaszyfrowane zapisz w archiwach w postaci odszyfrowanej

Ta opcja umożliwia określenie, czy pliki mają być odszyfrowane przed zapisaniem ich w archiwum kopii zapasowej.

Ustawienie wstępne: **Wyłączone**.

Zignoruj tę opcję, jeżeli nie korzystasz z szyfrowania. Włącz tę opcję, jeżeli kopia zapasowa zawiera pliki zaszyfrowane, które po odzyskaniu mają być dostępne dla dowolnego użytkownika. W przeciwnym razie tylko użytkownik, który zaszyfrował pliki lub foldery, będzie mógł je odczytać. Odszyfrowanie może być również przydatne, jeżeli odzyskanie zaszyfrowanych plików następuje na innym komputerze.

*Funkcja szyfrowania plików jest dostępna w systemach Windows używających systemu plików NTFS z systemem szyfrowania plików (Encrypting File System). Aby uzyskać dostęp do ustawień szyfrowania plików lub folderów, wybierz **Właściwości > Ogólne > Atrybuty zaawansowane > Szyfruj zawartość, aby zabezpieczyć dane.***

Zachowaj ustawienia zabezpieczeń plików w archiwach

Ta opcja pozwala określić, czy razem z kopią zapasową plików utworzyć również kopię zapasową uprawnień NTFS.

Ustawienie wstępne: **Włączone.**

Gdy opcja jest włączona, pliki i foldery są zapisywane w archiwum z oryginalnymi uprawnieniami odczytu, zapisu lub wykonywania plików każdego użytkownika lub grupy użytkowników. W przypadku odzyskiwania plików lub folderów na komputerze bez konta użytkownika określonego w uprawnieniach ich odczyt lub modyfikacja może okazać się niemożliwa.

Aby całkowicie wyeliminować ten problem, wyłącz zachowanie ustawień zabezpieczeń plików w archiwach. Odzyskane pliki i foldery zawsze otrzymają uprawnienia folderu, do którego zostaną odzyskane z dysku, jeżeli zostaną odzyskane do katalogu głównego.

Ewentualnie można wyłączyć odzyskiwanie (s. 138) ustawień zabezpieczeń, nawet jeżeli znajdują się w archiwum. Rezultat będzie taki sam — pliki otrzymają uprawnienia folderu nadrzędnego.

*Aby uzyskać dostęp do uprawnień NTFS pliku lub folderu, wybierz **Właściwości** > **Zabezpieczenia**.*

Komponenty na nośniku

Ta opcja jest dostępna w systemach operacyjnych Windows i Linux, gdy miejscem docelowym kopii zapasowej jest nośnik wymienny.

Podczas tworzenia kopii zapasowej na nośniku wymiennym można przekształcić ten nośnik w zwykły nośnik startowy (s. 424) oparty na systemie Linux, dopisując do niego dodatkowe komponenty. Wskutek tego oddzielny dysk ratunkowy nie będzie potrzebny.

Ustawienie wstępne: **Brak wyboru.**

Zaznacz pola wyboru komponentów, które chcesz umieścić na nośniku startowym:

- **One-Click Restore** (przywracanie jednym kliknięciem) to minimalny dodatek do kopii zapasowej dysku przechowywanej na nośniku wymiennym, który umożliwia łatwe odzyskiwanie danych z kopii zapasowej. Uruchomienie komputera z nośnika i kliknięcie **Uruchom Acronis One-click Restore** spowoduje natychmiastowe odzyskanie wszystkich danych w trybie dyskretnym do ich oryginalnej lokalizacji.

  Przestroga: *Ponieważ metoda przywracania jednym kliknięciem nie przewiduje ustawień wybieranych przez użytkownika, takich jak określenie odzyskiwanych woluminów, funkcja Acronis One-Click Restore powoduje zawsze odzyskanie danych z całego dysku. Jeśli dysk zawiera kilka woluminów i planujesz korzystanie z funkcji Acronis One-Click Restore, w kopii zapasowej uwzględnij wszystkie woluminy. Woluminy nieuwzględnione w kopii zapasowej zostaną utracone.*

- **Agent startowy** to ratunkowe narzędzie startowe (oparte na jądrze systemu Linux), które zawiera większość funkcji agenta programu Acronis Backup & Recovery 10 Umieszczając ten komponent na nośniku, uzyskasz więcej funkcji podczas odzyskiwania. Operację odzyskiwania będzie można skonfigurować w taki sam sposób jak w przypadku zwykłego nośnika startowego. Użyj funkcji Active Restore lub Universal Restore. Jeśli nośnik jest tworzony w systemie Windows dostępna będzie także funkcja zarządzania dyskiem.

Obsługa błędów

Te opcje są przeznaczone dla systemów operacyjnych Windows i Linux oraz nośników startowych.

Umożliwiają one określenie sposobu obsługi błędów, które mogą wystąpić podczas tworzenia kopii zapasowej.

Nie pokazuj komunikatów ani okien dialogowych podczas przetwarzania (tryb dyskretny)

Ustawienie wstępne: **Wyłączone**.

Po włączeniu trybu dyskretnego program automatycznie obsługuje sytuacje wymagające działania użytkownika (poza obsługą sektorów uszkodzonych, która jest zdefiniowana jako osobna opcja). Jeśli operacja nie może być kontynuowana bez działania użytkownika, zakończy się niepowodzeniem. Szczegółowe informacje na temat operacji, w tym błędy, które wystąpiły, można znaleźć w dzienniku operacji.

W przypadku wystąpienia błędu spróbuj ponownie

Ustawienie wstępne: **Włączone**. **Liczba ponawianych prób: 5. Odstęp między próbami: 30 sekund.**

Po wystąpieniu błędu, który można naprawić, program próbuje ponownie wykonać operację, która zakończyła się niepowodzeniem. Można ustawić odstęp pomiędzy kolejnymi próbami oraz ich liczbę. Ponowne próby zostaną wstrzymane po pomyślnym wykonaniu operacji LUB wykonaniu określonej liczby prób, w zależności od tego, który warunek zostanie spełniony wcześniej.

Jeśli na przykład docelowa lokalizacja kopii zapasowej w sieci będzie niedostępna, program będzie próbował nawiązać połączenie co 30 sekund, ale nie więcej niż 5 razy. Próby zostaną zakończone po wznowieniu połączenia LUB wykonaniu określonej liczby prób, w zależności od tego, który warunek zostanie spełniony wcześniej.

Ignoruj sektory uszkodzone

Ustawienie wstępne: **Wyłączone**.

Kiedy ta opcja jest wyłączona, po każdorazowym natrafieniu na sektor uszkodzony w programie otworzy się okno z prośbą o podjęcie decyzji, czy kontynuować czy zatrzymać procedurę tworzenia kopii zapasowej. Aby utworzyć kopię zapasową prawidłowych danych na szybko ginącym dysku, włącz ignorowanie sektorów uszkodzonych. Pozostałe dane zostaną skopiowane i można będzie zamontować wynikową kopię zapasową dysku i wyodrębnić prawidłowe pliki na innym dysku.

Dwa miejsca docelowe

Ta opcja jest dostępna w systemach operacyjnych Windows i Linux, gdy głównym miejscem docelowym kopii zapasowej jest *folder lokalny lub strefa Acronis Secure Zone*, a dodatkowym miejscem docelowym — *inny folder lokalny lub udział sieciowy.* Funkcji dodatkowego miejsca docelowego nie mogą pełnić skarbce zarządzane i serwery FTP.

Ustawienie wstępne: **Wyłączone**.

Gdy opcja dwóch miejsc docelowych jest włączona, agent automatycznie kopiuje każdą lokalnie tworzoną kopię zapasową w dodatkowym miejscu docelowym, na przykład w udziale sieciowym. Kiedy tworzenie kopii zapasowej w podstawowym miejscu docelowym dobiegnie końca, agent porównuje zaktualizowaną zawartość archiwum z zawartością archiwum dodatkowego oraz kopiuje w dodatkowe miejsce docelowe wszystkie brakujące kopie zapasowe wraz z nową kopią.

Ta opcja umożliwia szybkie utworzenie kopii zapasowej komputera na dysku wewnętrznym jako etap pośredni przed zapisaniem gotowej kopii zapasowej w sieci. Możliwość ta przydaje się w przypadku powolnych lub mocno obciążonych sieci i czasochłonnych procedur tworzenia kopii zapasowych. W przeciwieństwie do tworzenia kopii zapasowych bezpośrednio w lokalizacji zdalnej zerwanie połączenia w trakcie przesyłania kopii zapasowej nie wpłynie na operację jej tworzenia.

Inne korzyści:

- Replikacja zwiększa niezawodność archiwum.
- Użytkownicy mobilni mogą w trakcie podróży tworzyć kopie zapasowe danych z komputerów przenośnych w strefie Acronis Secure Zone. Gdy komputer przenośny zostanie podłączony do sieci firmowej, wszystkie zmiany wprowadzone w archiwum są przesyłane do archiwum stacjonarnego po pierwszej operacji tworzenia kopii zapasowej.

Gdy chroniona hasłem strefa Acronis Secure Zone zostanie wybrana jako podstawowe miejsce docelowe, należy pamiętać, że archiwum w miejscu dodatkowym nie będzie chronione hasłem.

Aby użyć dwóch miejsc docelowych:

1. Zaznacz pole wyboru **Użyj dwóch miejsc docelowych**.
2. Wyszukaj dodatkowe miejsce docelowe lub ręcznie wprowadź pełną ścieżkę do niego.
3. Kliknij **OK**.

Może być konieczne podanie poświadczeń dostępu do dodatkowego miejsca docelowego. GWprowadź poświadczenia po wyświetleniu monitu.

Warunki uruchomienia zadania

Ta opcja jest uwzględniana w systemach operacyjnych Windows i Linux.

Jest ona niedostępna podczas pracy z nośnikiem startowym.

Ta opcja określa działanie programu tuż przed uruchomieniem zadania tworzenia kopii zapasowej (zbliża się zaplanowany termin lub występuje zdarzenie określone w harmonogramie), kiedy warunek (lub jeden z wielu warunków) nie został spełniony. Więcej informacji na temat warunków można znaleźć w częściach Planowanie (s. 185) i Warunki (s. 197).

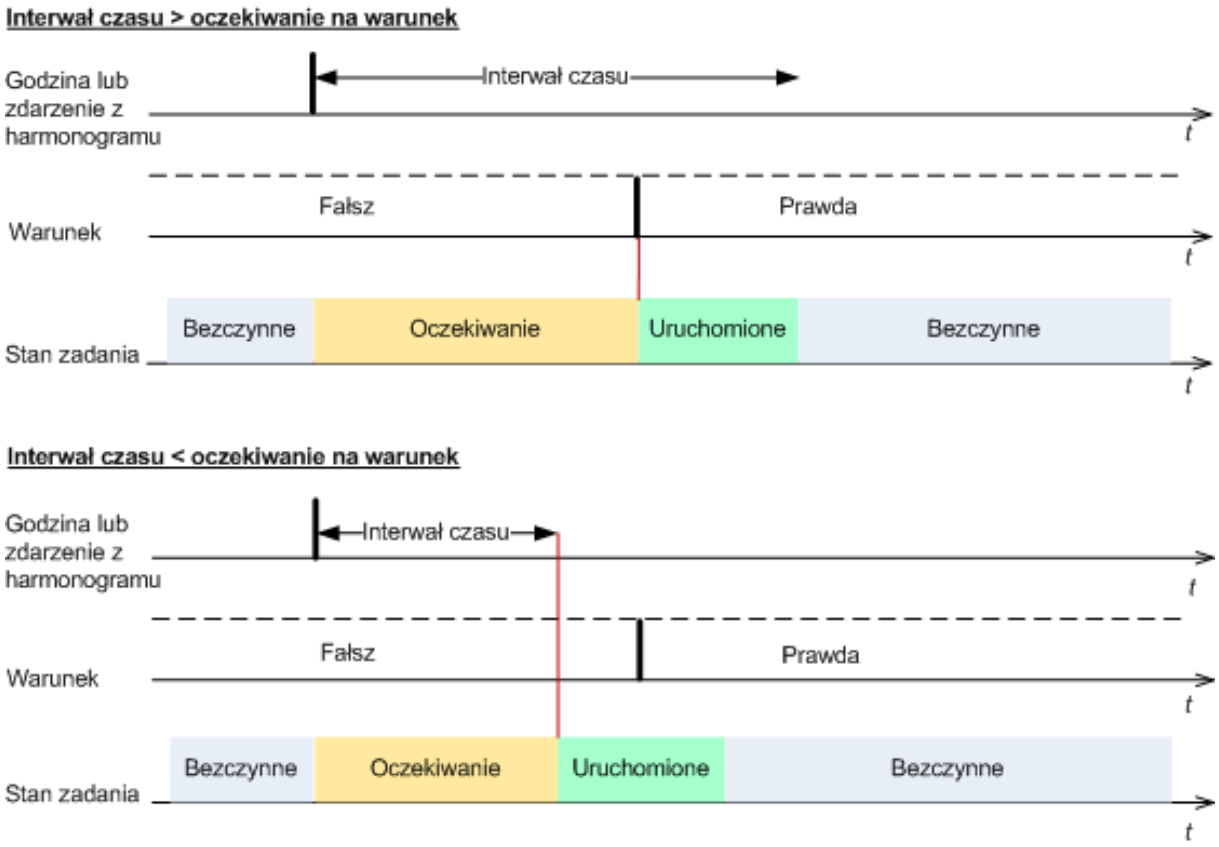
Ustawienie wstępne: **Poczekaj na spełnienie warunków.**

Poczekaj na spełnienie warunków

Przy tym ustawieniu funkcja harmonogramu spowoduje rozpoczęcie monitorowania warunków i uruchomienie zadania, kiedy tylko warunki zostaną spełnione. Jeżeli warunki nie zostaną w ogóle spełnione, zadanie nie zostanie uruchomione.

Jeśli warunki nie są spełnione przez dłuższy czas, a dalsze opóźnianie utworzenia kopii zapasowej jest ryzykowne, można wyznaczyć okres czasu, po upływie którego zadanie zostanie uruchomione niezależnie od spełnienia warunku. Zaznacz pole wyboru **Uruchom zadanie mimo to po upływie** i określ czas. Zadanie zostanie uruchomione, kiedy tylko warunki zostaną spełnione LUB maksymalny czas opóźnienia upłynie, w zależności od tego, który warunek zostanie spełniony wcześniej.

Wykres czasu: Poczekaj na spełnienie warunków



Pomiń wykonywanie zadania

Opóźnianie tworzenia kopii zapasowej jest niedopuszczalne na przykład wówczas, gdy istnieje konieczność utworzenia kopii zapasowej dokładnie o określonej godzinie. Wówczas sensowne jest

pominięcie tworzenia kopii zapasowej, a nie czekanie na spełnienie warunków, szczególnie jeżeli zdarzenia następują relatywnie często.

Obsługa niepowodzenia zadania

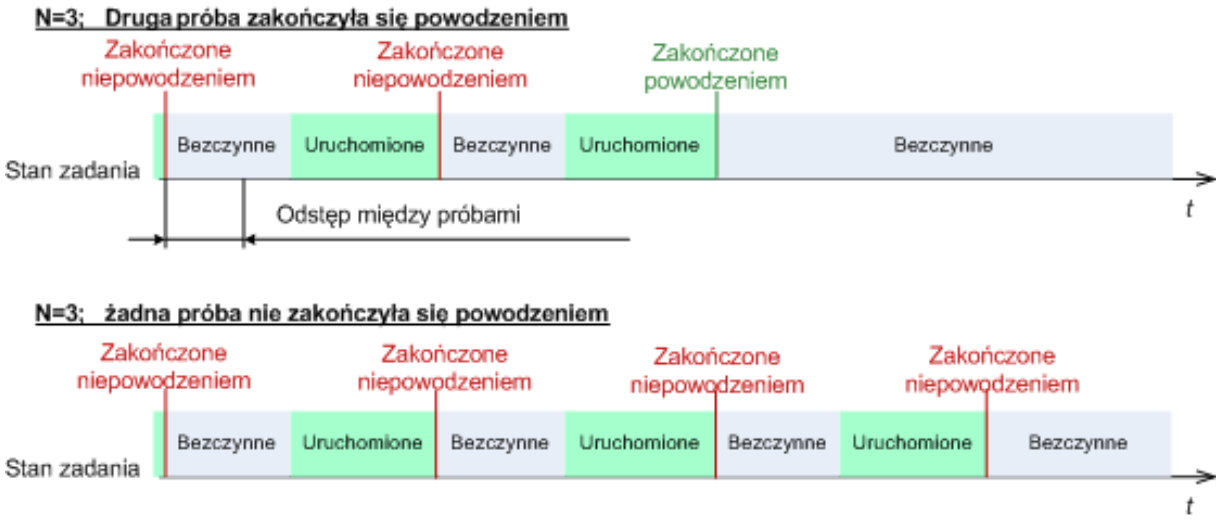
Ta opcja jest dostępna w systemach operacyjnych Windows i Linux.

Jest ona niedostępna podczas pracy z nośnikiem startowym.

Opcja określa zachowanie programu, gdy nie powiedzie się wykonanie dowolnego zadania z planu tworzenia kopii zapasowych.

Ustawieniem wstępnym jest **brak ponownego uruchamiania zadania zakończonego niepowodzeniem.**

Program ponowi próbę wykonania zadania zakończonego niepowodzeniem, jeśli zostało zaznaczone pole wyboru **Ponownie uruchom zadanie zakończone niepowodzeniem** oraz została określona liczba prób i odstęp czasowy między nimi. Program wstrzyma próby, gdy jedna z nich zakończy się powodzeniem LUB po wykonaniu określonej liczby prób, w zależności od tego, który z tych warunków zostanie spełniony wcześniej.



Jeśli zadanie zakończy się niepowodzeniem z powodu błędu w planie tworzenia kopii zapasowych, można zmodyfikować plan, jeśli zadanie jest w stanie bezczynności. Jeśli zadanie jest uruchomione, należy je zatrzymać, a następnie przystąpić do modyfikacji planu tworzenia kopii zapasowych.

Obsługa taśmy

Opcje te są uwzględniane, gdy miejscem docelowym kopii zapasowej jest skarbiec zarządzany znajdujący się w bibliotece taśm.

Opcje **Obsługa taśmy** umożliwiają określenie sposobu dystrybucji kopii zapasowych na taśmach przez zadania tworzenia kopii zapasowych.

Niektóre kombinacje opcji dotyczących taśm mogą powodować zmniejszenie efektywności wykorzystania całej biblioteki lub poszczególnych taśm. Jeśli zmodyfikowanie tych opcji nie jest konieczne, należy pozostawić je bez zmian.

Archiwum może zajmować kilka taśm. Do przechowywania danych kopii zapasowych jest wtedy używany tzw. **zestaw taśm**.

Zestaw taśm jest to logiczna grupa składająca się z jednej lub kilku taśm zawierających kopie zapasowe określonych chronionych danych. Zestaw taśm może również zawierać kopie zapasowe innych danych.

Osobny zestaw taśm jest to zestaw zawierający tylko kopie zapasowe określonych chronionych danych. Nie można na nim zapisać innych kopii zapasowych.

(Dla tworzonej zasady/planu tworzenia kopii zapasowych) Użyj osobnego zestawu taśm

Ustawienie wstępne: **Wyłączone**.

Jeśli użytkownik nie zmieni tej opcji, kopie zapasowe należące do tworzonej zasady lub planu tworzenia kopii zapasowych można zapisywać na taśmach zwierających inne kopie zapasowe utworzone z danych z innych komputerów. Również kopie zapasowe utworzone przez inne zasady można zapisywać na taśmach zawierających kopie zapasowe utworzone przez daną zasadę. Nie ma problemu z takimi taśmami, ponieważ program wszystkimi taśmami zarządza automatycznie.

Po włączeniu tej opcji kopie zapasowe należące do tworzonej zasady lub planu tworzenia kopii zapasowych będą zapisywane na osobnym zestawie taśm, na którym nie będą zapisywane inne kopie zapasowe.

Gdy konsola jest podłączona do serwera zarządzania

Opcja **Użyj osobnego zestawu taśm** ma bardziej dokładną definicję. Dlatego w tworzonej zasadzie tworzenia kopii zapasowych można użyć osobnego zestawu taśm dla wszystkich komputerów lub dla każdego komputera osobno.

Opcja **Jeden zestaw taśm dla wszystkich komputerów** jest domyślnie wybrana. Ogólnie rzecz biorąc, opcja ta umożliwia bardziej efektywne wykorzystanie taśm niż opcja **Oddzielny zestaw taśm dla każdego komputera**. Jednak ta druga opcja może być przydatna, gdy na przykład istnieją specjalne wymagania dotyczące przechowywania taśm z kopiami zapasowymi danego komputera w innej lokalizacji.

Po włączeniu opcji **Użyj osobnego zestawu taśm** może wystąpić sytuacja, w której program chce zapisać kopię zapasową na taśmie, która aktualnie jest wyjęta z urządzenia biblioteki taśm. Należy określić sposób postępowania w takiej sytuacji.

- **Poproś o działanie użytkownika** — zadanie tworzenia kopii zapasowej przejdzie w stan **Wymagające działania** i będzie czekało na załadowanie do urządzenia biblioteki taśmy o odpowiedniej etykiecie.
- **Użyj wolnej taśmy** — program zapisze kopię zapasową na wolnej taśmie, dlatego operacja będzie wstrzymana tylko, gdy w bibliotece nie ma wolnych taśm.

Zawsze używaj wolnej taśmy

Jeśli użytkownik nie zmieni poniższych opcji, wszystkie kopie zapasowe będą zapisywane na taśmie określonej w opcji **Użyj osobnego zestawu taśm**. Po włączeniu niektórych z poniższych opcji program będzie dodawał nowe taśmy do zestawu taśm podczas każdej operacji tworzenia pełnej, przyrostowej lub różnicowej kopii zapasowej.

- **Do każdej pełnej kopii zapasowej**

Ustawienie wstępne: **Wyłączone**.

Po włączeniu tej opcji program zapisuje wszystkie pełne kopie zapasowe na wolnych taśmach. Taśma jest specjalnie ładowana do tej operacji. Gdy opcja **Użyj osobnego zestawu taśm** jest włączona, program może dodać do taśmy tylko przyrostowe lub różnicowe kopie zapasowe tych samych danych.

- **Dla każdej różnicowej kopii zapasowej**

Ustawienie wstępne: **Wyłączone**.

Gdy ta opcja jest włączona, program zapisuje wszystkie różnicowe kopie zapasowe na wolnych taśmach. Ta opcja jest dostępna tylko, gdy dla wszystkich pełnych kopii zapasowych program używa wolnych taśm.

- **Do każdej przyrostowej kopii zapasowej**

Ustawienie wstępne: **Wyłączone**.

Gdy ta opcja jest włączona, program zapisuje wszystkie przyrostowe kopie zapasowe na wolnych taśmach. Ta opcja jest dostępna tylko, gdy dla wszystkich pełnych i różnicowych kopii zapasowych program używa wolnych taśm.

Ustawienia dodatkowe

Określ dodatkowe ustawienia operacji tworzenia kopii zapasowej, zaznaczając lub czyszcząc poniższe pola wyboru.

Zastąp dane na taśmie bez monitowania użytkownika o potwierdzenie

Ta opcja jest dostępna tylko podczas tworzenia kopii zapasowej w urządzeniu taśmowym.

Ustawienie wstępne: **Wyłączone**.

Rozpoczynając tworzenie kopii zapasowej na niecałkowicie pustej taśmie w lokalnie podłączonym urządzeniu taśmowym, program wyświetli ostrzeżenie, że za chwilę nastąpi utrata danych na taśmie. Aby wyłączyć to ostrzeżenie, zaznacz to pole wyboru.

Odmontuj nośnik po utworzeniu kopii zapasowej

Ta opcja jest dostępna w systemach operacyjnych Windows i Linux.

Jest ona dostępna podczas tworzenia kopii zapasowej na nośniku wymiennym (płyta CD lub DVD, taśma albo dyskietka).

Ustawienie wstępne: **Wyłączone**.

Po utworzeniu kopii zapasowej może nastąpić wysunięcie docelowej płyty CD lub DVD albo odmontowanie taśmy.

W przypadku tworzenia kopii zapasowej na nośnikach wymiennych zapytaj o pierwszy nośnik

Ta opcja jest dostępna tylko podczas tworzenia kopii zapasowej na nośniku wymiennym.

Określa ona, czy podczas tworzenia kopii zapasowej na nośniku wymiennym ma być wyświetlany monit **Włóż pierwszy nośnik**.

Ustawienie wstępne: **Włączone**.

Gdy opcja jest włączona, a użytkownik nie znajduje się w pobliżu komputera, utworzenie kopii zapasowej na nośniku wymiennym może okazać się niemożliwe, ponieważ program będzie czekał na kliknięcie przycisku OK w oknie monitu. Dlatego, jeśli planujesz w harmonogramie tworzenie kopii zapasowej na nośniku wymiennym, wyłącz wyświetlanie monitu. W takiej sytuacji, jeśli nośnik wymienny będzie dostępny (na przykład włożona będzie płyta DVD), zadanie będzie kontynuowane bez udziału użytkownika.

Resetuj bit archiwum

Ta opcja jest dostępna tylko w przypadku kopii zapasowej na poziomie plików w systemach operacyjnych Windows i na nośniku startowym.

Ustawienie wstępne: **Wyłączone**.

W systemach operacyjnych Windows każdy plik ma atrybut **Plik jest gotowy do archiwizacji**, dostępny po wybraniu **Plik** -> **Właściwości** -> **Ogólne** -> **Zaawansowane** -> **Atrybuty archiwizacji i indeksowania**. W systemie operacyjnym ten atrybut — zwany również bitem archiwum — jest ustawiany przy każdej zmianie pliku, a aplikacje do tworzenia kopii zapasowych mogą go przestawiać za każdym razem, gdy umieszczają plik w kopii zapasowej. Wartość bitu archiwum jest używana przez różne aplikacje, na przykład bazy danych.

Gdy pole wyboru **Resetuj bit archiwum** jest zaznaczone, program Acronis Backup & Recovery 10 zresetuje bity archiwum wszystkich plików umieszczanych w kopii zapasowej. Program Acronis Backup & Recovery 10 sam w sobie nie korzysta z wartości bitu archiwum. Podczas tworzenia przyrostowej lub różnicowej kopii zapasowej program ustala, czy plik się nie zmienił, na podstawie rozmiaru pliku i daty/godziny jego ostatniego zapisu.

Ponownie uruchom komputer po utworzeniu kopii zapasowej

Ta opcja jest dostępna tylko podczas pracy z nośnikiem startowym.

Ustawienie wstępne: **Wyłączone**.

Gdy opcja jest włączona, po utworzeniu kopii zapasowej program Acronis Backup & Recovery 10 ponownie uruchomi komputer.

Jeśli na przykład komputer jest domyślnie uruchamiany z dysku twardego i to pole jest zaznaczone, niezwłocznie po utworzeniu kopii zapasowej przez agenta komputer zostanie ponownie uruchomiony i rozpocznie się ładowanie systemu operacyjnego.

Deduplikuj kopie zapasowe po przetransferowaniu ich do skarbca (nie deduplikuj w miejscu źródłowym)

Ta opcja jest dostępna tylko w zaawansowanych wersjach programu Acronis Backup & Recovery 10.

Ta opcja jest dostępna w przypadku systemów operacyjnych Windows i Linux oraz nośnika startowego, gdy miejscem docelowym kopii zapasowej jest skarbiec deduplikacji.

Ustawienie wstępne: **Wyłączone**.

Włączenie tej opcji powoduje wyłączenie deduplikacji kopii zapasowych w źródle, co oznacza, że deduplikacja będzie wykonywana w węźle magazynowania Acronis Backup & Recovery 10 Storage Node po zapisaniu kopii zapasowej w skarbcu (jest to czynność nazywana deduplikacją w miejscu docelowym).

Wyłączenie deduplikacji w źródle może przyspieszyć tworzenie kopii zapasowych, ale jednocześnie spowodować większy ruch w sieci i obciążenie węzła magazynowania. Ostateczny rozmiar kopii zapasowej w skarbcu jest niezależny od tego, czy deduplikacja w źródle jest włączona.

Opis deduplikacji w źródle i deduplikacji w miejscu docelowym znajduje się w sekcji Omówienie deduplikacji (s. 81).

Razem z kopiami zapasowymi zapisz metadane programowej macierzy RAID i woluminu LVM

Ta opcja jest dostępna tylko w przypadku kopii zapasowych komputerów z systemem Linux tworzonych na poziomie dysku.

Ustawienie wstępne: **Włączone**.

Gdy opcja jest włączona, przed utworzeniem kopii zapasowej program Acronis Backup & Recovery 10 zapisze w katalogu **/etc/Acronis** informacje o strukturze woluminów logicznych (woluminów LVM) oraz programowych macierzy RAID systemu Linux (urządzeń MD).

Podczas odzyskiwania urządzeń MD i woluminów LVM za pomocą nośnika startowego informacji tych można użyć do automatycznego odtworzenia struktury woluminów. Aby uzyskać instrukcje, zobacz Odzyskiwanie urządzeń MD i woluminów logicznych (s. 304).

Po wybraniu tej opcji upewnij się, że w woluminach wybranych do utworzenia kopii zapasowej znajduje się wolumin z katalogiem **/etc/Acronis**.

Użyj usługi FTP w trybie aktywnym

Ustawienie wstępne: **Wyłączone**.

Włącz tę opcję, jeśli serwer FTP obsługuje tryb aktywny i chcesz go używać do przesyłania plików.

3.4.2 Domyślne opcje odzyskiwania

Każdy agent Acronis ma własne domyślne opcje odzyskiwania. Po zainstalowaniu agenta domyślne opcje mają określone wartości, które w dokumentacji są nazywane **wstępnie zdefiniowanymi wartościami**. Podczas tworzenia zadania odzyskiwania można zastąpić wartość domyślną opcji wartością niestandardową, której program ma użyć w tym konkretnym zadaniu.

Można również dostosować opcję domyślną, zmieniając jej wartość na inną niż wstępnie zdefiniowana. Program będzie domyślnie używał nowej wartości we wszystkich zadaniach odzyskiwania utworzonych na danym komputerze.

Aby wyświetlić i zmienić domyślne opcje odzyskiwania, połącz konsolę z zarządzanym komputerem i z górnego menu wybierz **Opcje > Domyślne opcje tworzenia kopii zapasowej i odzyskiwania > Domyślne opcje odzyskiwania**.

Dostępne opcje odzyskiwania

Zakres dostępnych opcji odzyskiwania zależy od następujących czynników:

- środowisko, w którym działa agent (Windows, Linux, nośnik startowy);
- typ odzyskiwanych danych (dysk, plik);
- system operacyjny odzyskiwany z kopii zapasowej dysku (Windows, Linux).

W poniższej tabeli zestawiono dostępność opcji odzyskiwania.

	Agent dla systemu Windows		Agent dla systemu Linux		Nośnik startowy (w systemie Linux lub środowisku PE)	
	Odzyskiwanie dysków	Odzyskiwanie plików	Odzyskiwanie dysków	Odzyskiwanie plików	Odzyskiwanie dysków	Odzyskiwanie plików

		(również z kopii zapasowej dysku)		**(również z kopii zapasowej dysku)**		**(również z kopii zapasowej dysku)**
Polecenia poprzedzające odzyskiwanie/następujące po nim (s. 136)	+	+	+	+	Tylko PE	Tylko PE
Priorytet odzyskiwania (s. 137)	+	+	+	+	—	—
Zabezpieczenia na poziomie plików (s. 138):						
Odzyskaj pliki z ich ustawieniami zabezpieczeń	—	+	—	+	—	+
Obsługa błędów (s. 141):						
Nie pokazuj komunikatów ani okien dialogowych podczas przetwarzania (tryb dyskretny)	+	+	+	+	+	+
W przypadku wystąpienia błędu spróbuj ponownie	+	+	+	+	+	+
Ustawienia dodatkowe (s. 141):						
Ustaw bieżącą datę i godzinę odzyskiwanych plików	—	+	—	+	—	+
Sprawdź poprawność archiwum przed odzyskaniem	+	+	+	+	+	+
Sprawdź system plików po odzyskaniu	+	—	+	—	+	—
Automatycznie ponownie uruchom komputer, gdy wymaga tego proces odzyskiwania	+	+	+	+	—	—
Zmień identyfikator SID po odzyskiwaniu	Odzyskiwanie systemu Windows	—	Odzyskiwanie systemu Windows	—	Odzyskiwanie systemu Windows	—
Powiadomienia:						
Wiadomości e-mail (s. 138)	+	+	+	+	—	—
Komunikaty wyskakujące w systemie Windows (s. 139)	+	+	+	+	—	—
Śledzenie zdarzeń:						
Dziennik zdarzeń systemu Windows (s. 140)	+	+	—	—	—	—
SNMP (s. 140)	+	+	+	+	—	—

Polecenia poprzedzające/następujące

Ta opcja ma zastosowanie w systemach operacyjnych Windows i Linux oraz w przypadku nośników startowych opartych na środowisku PE.

Ta opcja umożliwia określenie poleceń wykonywanych automatycznie przed odzyskiwaniem danych i po jego zakończeniu.

Przykład zastosowania poleceń poprzedzających/następujących:

- uruchomienie polecenia `Checkdisk` w celu znalezienia i naprawienia problemów logicznych z systemem plików, błędów fizycznych lub sektorów uszkodzonych przed rozpoczęciem odzyskiwania lub po jego zakończeniu.

Program nie obsługuje poleceń interaktywnych wymagających działania użytkownika (na przykład „pause").

Polecenia po zakończeniu odzyskiwania nie zostaną wykonane, jeśli proces odzyskiwania uruchomi ponownie komputer.

Aby określić polecenia poprzedzające/następujące

1. Włącz wykonywanie poleceń poprzedzających/następujących, zaznaczając następujące opcje:
   - **Wykonaj przed odzyskiwaniem**
   - **Wykonaj po odzyskiwaniu**
2. Wykonaj jedną z następujących czynności:
   - Kliknij **Edytuj**, aby określić nowe polecenie lub plik wsadowy.
   - Wybierz istniejące polecenie lub plik wsadowy z listy rozwijanej.
3. Kliknij **OK**.

Polecenie poprzedzające odzyskiwanie

Aby określić polecenie/plik wsadowy do wykonania przed rozpoczęciem procesu odzyskiwania

1. W polu **Polecenie** wpisz polecenie lub wskaż plik wsadowy. Program nie obsługuje poleceń interaktywnych, to znaczy poleceń wymagających działania użytkownika (na przykład „pause".)
2. W polu **Katalog roboczy** określ ścieżkę do katalogu, w którym zostanie wykonane polecenie lub plik wsadowy.
3. W polu **Argumenty** określ argumenty wykonywania polecenia, jeśli są wymagane.
4. W zależności od wyniku, który chcesz uzyskać, wybierz odpowiednie opcje opisane w poniższej tabeli.
5. Kliknij **Testuj polecenie**, aby sprawdzić, czy polecenie jest prawidłowe.

Pole wyboru	**Wybór**			
Zakończ zadanie niepowodzeniem, jeśli wykonanie polecenia się nie powiedzie	Wybrane	Niewybrane	Wybrane	Niewybrane
Nie przeprowadzaj odzyskiwania przed zakończeniem wykonywania polecenia	Wybrane	Wybrane	Niewy-brane	Niewybrane

Wynik				
	Ustawienie wstępne Przeprowadź odzyskiwanie tylko pomyślnym wykonaniu polecenia. Zakończ zadanie niepowodzeniem, jeśli wykonanie polecenia się nie powiedzie.	Przeprowadź odzyskiwanie po wykonaniu polecenia, niezależnie od tego, czy zakończyło się powodzeniem, czy niepowodzeniem.	N/D	Przeprowadź odzyskiwanie równolegle z wykonywaniem polecenia i niezależnie od wyniku jego wykonania.

Polecenie po zakończeniu odzyskiwania

Aby określić polecenie/plik wykonywalny, które mają zostać wykonane po zakończeniu odzyskiwania

1. W polu **Polecenie** wpisz polecenie lub wskaż plik wsadowy.
2. W polu **Katalog roboczy** określ ścieżkę do katalogu, w którym zostanie wykonane polecenie lub plik wsadowy.
3. W polu **Argumenty** określ argumenty wykonywania polecenia, jeśli są wymagane.
4. Jeśli pomyślne wykonanie polecenia ma znaczenie krytyczne, zaznacz pole wyboru **Zakończ zadanie niepowodzeniem, jeśli wykonanie polecenia się nie powiedzie**. W razie niepowodzenia wykonania polecenia wynik uruchomienia zadania zostanie również ustawiony na Zakończone niepowodzeniem.

   Jeśli to pole wyboru nie jest zaznaczone, wynik wykonania polecenia nie wpływa na powodzenie lub niepowodzenie wykonania zadania. Wynik wykonania polecenia można sprawdzić w dzienniku lub na liście Błędy i ostrzeżenia wyświetlonej na **Pulpicie nawigacyjnym**.
5. Kliknij **Testuj polecenie**, aby sprawdzić, czy polecenie jest prawidłowe.

Polecenia po zakończeniu odzyskiwania nie zostaną wykonane, jeśli proces odzyskiwania uruchomi ponownie komputer.

Priorytet odzyskiwania

Ta opcja jest uwzględniana w systemach operacyjnych Windows i Linux.

Jest ona niedostępna podczas pracy z nośnikiem startowym.

Priorytet procesu uruchomionego w systemie określa ilość zasobów procesora i zasobów systemowych przydzielonych do tego procesu. Zmniejszenie priorytetu odzyskiwania spowoduje zwolnienie większej ilości zasobów dla innych aplikacji. Zwiększenie priorytetu odzyskiwania może spowodować przyspieszenie tego procesu, ponieważ wymaga od systemu przydzielenia większej ilości zasobów do aplikacji, która przeprowadza odzyskiwanie. Jednak ostateczny efekt zależy od całkowitego wykorzystania procesora oraz innych czynników, takich jak szybkość operacji wejścia/wyjścia na dysku i ruch w sieci.

Ustawienie wstępne: **Normalny**.

Aby określić priorytet procesu odzyskiwania

Wybierz jedno z następujących ustawień:

- **Niski** — aby zminimalizować ilość zasobów wykorzystywanych przez proces odzyskiwania, pozostawiając więcej zasobów dla innych procesów uruchomionych na komputerze;

- **Normalny** — aby uruchamiać proces odzyskiwania z normalną szybkością, przydzielając zasoby na równi z innymi procesami;
- **Wysoki** — aby zmaksymalizować szybkość procesu odzyskiwania, odbierając zasoby innym procesom.

Zabezpieczenia na poziomie plików

Ta opcja ma zastosowanie tylko w przypadku odzyskiwania z kopii zapasowej plików systemu Windows na poziomie pliku.

Ta opcja określa, czy razem z plikami mają być odzyskiwane uprawnienia NTFS do plików.

Ustawienie wstępne: **Odzyskaj pliki z ich ustawieniami zabezpieczeń**.

Jeśli uprawnienia NTFS zostały zachowane podczas tworzenia kopii zapasowej (s. 126), można wybrać, czy mają one być odzyskiwane, czy też pliki powinny dziedziczyć uprawnienia NTFS z folderu, do którego są odzyskiwane.

Powiadomienia

Program Acronis Backup & Recovery 10 umożliwia powiadamianie użytkowników o zakończeniu odzyskiwania pocztą e-mail lub za pomocą usługi komunikatów.

Poczta e-mail

Ta opcja ma zastosowanie w systemach operacyjnych Windows i Linux.

Ta opcja jest niedostępna podczas wykonywania operacji na nośnikach startowych.

Opcja umożliwia otrzymywanie pocztą e-mail powiadomień o pomyślnym zakończeniu lub niepowodzeniu zadania odzyskiwania albo konieczności wykonania działań wraz z pełnym dziennikiem zadania.

Ustawienie wstępne: **Wyłączone**.

Aby skonfigurować powiadamianie pocztą e-mail

1. Zaznacz pole wyboru **Wysyłaj powiadomienia pocztą e-mail**, aby włączyć powiadamianie.
2. W polu **Adresy e-mail** wpisz adresy e-mail, na które chcesz wysłać powiadomienia. Możesz wpisać kilka adresów rozdzielonych średnikami.
3. W sekcji **Wysyłaj powiadomienia** zaznacz odpowiednie pola wyboru
   - **Po pomyślnym utworzeniu kopii zapasowej** — aby wysłać powiadomienia po pomyślnym utworzeniu kopii zapasowej
   - **Gdy utworzenie kopii zapasowej się nie powiedzie** — aby wysłać powiadomienia, gdy utworzenie kopii zapasowej nie powiedzie się

   Pole wyboru **Gdy jest konieczne działanie użytkownika** jest zawsze zaznaczone.
4. Aby wiadomość e-mail zawierała wpisy dziennika związane z tworzeniem kopii zapasowej, zaznacz pole wyboru **Dodaj do powiadomienia pełny dziennik**.
5. Kliknij **Dodatkowe parametry poczty e-mail**, aby skonfigurować przedstawione poniżej parametry poczty e-mail, a następnie kliknij **OK**:
   - **Od** — wpisz adres e-mail użytkownika, który będzie nadawcą wiadomości. Jeśli to pole pozostanie puste, w polu nadawcy program wpisze adresata wiadomości.
   - **Użyj szyfrowania** — umożliwia włączenie szyfrowanego połączenia z serwerem poczty. Można wybrać szyfrowanie SSL lub TLS.

- Niektórzy dostawcy usług internetowych wymagają uwierzytelniania na serwerze poczty przychodzącej przed umożliwieniem wysłania wiadomości. Jeśli tak jest, zaznacz pole wyboru **Zaloguj się na serwerze poczty przychodzącej**, aby umożliwić używanie serwera POP i skonfigurować jego ustawienia:
  - **Serwer poczty przychodzącej (POP)** — wprowadź nazwę serwera POP.
  - **Port** — ustaw port serwera POP. Domyślnie jest ustawiony port 110.
  - **Nazwa użytkownika** — wprowadź nazwę użytkownika.
  - **Hasło** — wprowadź hasło.
- Zaznacz pole wyboru **Użyj określonego serwera poczty wychodzącej**, aby umożliwić używanie serwera SMTP i skonfigurować jego ustawienia:
  - **Serwer poczty wychodzącej (SMTP)** — wprowadź nazwę serwera SMTP.
  - **Port** — ustaw port serwera SMTP. Domyślnie jest ustawiony port 25.
  - **Nazwa użytkownika** — wprowadź nazwę użytkownika.
  - **Hasło** — wprowadź hasło.

Kliknij **Wyślij próbną wiadomość e-mail**, aby sprawdzić, czy ustawienia są poprawne.

Usługa Messenger (WinPopup)

Ta opcja ma zastosowanie w systemach operacyjnych Windows i Linux.

Opcja jest niedostępna podczas wykonywania operacji na nośnikach startowych.

Opcja umożliwia otrzymywanie powiadomień WinPopup o pomyślnym zakończeniu lub niepowodzeniu zadania albo konieczności wykonania działań.

Ustawienie wstępne: **Wyłączone**.

Przed skonfigurowaniem powiadomień WinPopup należy dopilnować, aby usługa Messenger była włączona na obu komputerach: wykonującym zadanie i odbierającym wiadomości.

Usługa Messenger nie jest domyślnie uruchamiana w systemach z grupy Microsoft Windows Server 2003. Zmień tryb uruchamiania usługi na Automatyczny i uruchom usługę.

Aby skonfigurować powiadomienia WinPopup:

1. Zaznacz pole wyboru **Wysyłaj powiadomienia WinPopup**.
2. W polu **Nazwa komputera** wprowadź nazwę komputera, do którego chcesz przesyłać powiadomienia. Używanie kilku nazw nie jest obsługiwane.
3. W sekcji **Wysyłaj powiadomienia** zaznacz odpowiednie pola wyboru
   - **Po pomyślnym odzyskaniu danych** — aby wysyłać powiadomienie po pomyślnym zakończeniu zadania odzyskiwania;
   - **Gdy odzyskanie danych się nie powiedzie** — aby wysyłać powiadomienie, gdy zadanie odzyskiwania się nie powiedzie.

   Pole wyboru **Gdy jest konieczne działanie użytkownika** — aby podczas operacji wysyłać powiadomienie, gdy jest wymagane działanie użytkownika — jest zawsze zaznaczone.
4. Kliknij **Wyślij próbny komunikat WinPopup**, aby sprawdzić, czy ustawienia są poprawne.

Śledzenie zdarzeń

Zdarzenia dziennika operacji odzyskiwania wykonywanych na komputerze zarządzanym można duplikować w dzienniku zdarzeń aplikacji systemu Windows. Można również wysyłać zdarzenia do określonych menedżerów SNMP.

Dziennik zdarzeń systemu Windows

Ta opcja ma zastosowanie tylko w systemie operacyjnym Windows.

Ta opcja jest niedostępna podczas wykonywania operacji na nośnikach startowych.

Opcja określa, czy agenty działające na komputerze zarządzanym muszą rejestrować zdarzenia operacji odzyskiwania w dzienniku zdarzeń aplikacji systemu Windows (aby wyświetlić ten dziennik, należy uruchomić plik **eventvwr.exe** lub wybrać polecenia **Panel sterowania > Administrative tools (Narzędzia administracyjne) > Event Viewer (Podgląd zdarzeń)**). Zdarzenia do rejestrowania można filtrować.

Ustawienie wstępne: **Użyj ustawień określonych w obszarze Opcje komputera**.

Aby wybrać, czy zdarzenia operacji odzyskiwania mają być rejestrowane w dzienniku zdarzeń aplikacji systemu Windows:

Wybierz jedno z następujących ustawień:

- **Użyj ustawień określonych w obszarze Opcje komputera** — aby używać ustawienia określonego dla komputera. Aby uzyskać więcej informacji, zobacz Opcje komputera (s. 105).
- **Rejestruj zdarzenia następujących typów** — aby rejestrować zdarzenia operacji odzyskiwania w dzienniku zdarzeń aplikacji. Należy określić typy zdarzeń, które mają być rejestrowane:
  - **Wszystkie zdarzenia** — rejestrowanie wszystkich zdarzeń (informacje, ostrzeżenia i błędy);
  - **Błędy i ostrzeżenia;**
  - **Tylko błędy.**
- **Nie rejestruj** — wyłączanie rejestrowania zdarzeń operacji odzyskiwania w dzienniku zdarzeń aplikacji.

Powiadomienia SNMP

Ta opcja ma zastosowanie zarówno w systemach operacyjnych Windows, jak i Linux.

Ta opcja jest niedostępna podczas wykonywania operacji na nośnikach startowych.

Opcja określa, czy agenty działające na komputerze zarządzanym muszą wysyłać zdarzenia dziennika operacji odzyskiwania do określonych menedżerów SNMP (Simple Network Management Protocol). Można wybrać typy zdarzeń, które będą wysyłane.

Aby uzyskać szczegółowe informacje na temat programu Acronis Backup & Recovery 10, zobacz „Obsługa SNMP (s. 59)”.

Ustawienie wstępne: **Użyj ustawień określonych w obszarze Opcje komputera**.

Aby wybrać, czy zdarzenia operacji odzyskiwania mają być wysyłane do menedżerów SNMP:

Wybierz jedno z następujących ustawień:

- **Użyj ustawień określonych w obszarze Opcje komputera** — aby używać ustawienia określonego dla komputera. Aby uzyskać więcej informacji, zobacz Opcje komputera (s. 105).

- **Wyślij osobne powiadomienie SNMP w przypadku każdego zdarzenia odzyskiwania** — aby wysyłać zdarzenia operacji odzyskiwania do określonych menedżerów SNMP.
  - **Typy wysyłanych zdarzeń** — wybierz typy zdarzeń, które będą wysyłane: **Wszystkie zdarzenia**, **Błędy i ostrzeżenia** lub **Tylko błędy**.
  - **Nazwa/adres IP serwera** — wpisz nazwę lub adres IP hosta z uruchomioną aplikacją do zarządzania SNMP, do której będą wysyłane komunikaty.
  - **Społeczność** — wpisz nazwę społeczności SNMP, do której należy aplikacja do zarządzania SNMP i komputer wysyłający. Typową społecznością jest „publiczna”.

  Kliknij **Wyślij wiadomość próbną**, aby sprawdzić, czy ustawienia są poprawne.
- **Nie wysyłaj powiadomień SNMP** — aby wyłączyć wysyłanie zdarzeń dziennika operacji odzyskiwania do menedżerów SNMP.

Obsługa błędów

Te opcje są przeznaczone dla systemów operacyjnych Windows i Linux oraz nośników startowych.

Umożliwiają one określenie sposobu obsługi błędów, które mogą wystąpić podczas odzyskiwania.

Nie pokazuj komunikatów ani okien dialogowych podczas przetwarzania (tryb dyskretny)

Ustawienie wstępne: **Wyłączone**.

Po włączeniu trybu dyskretnego program automatycznie obsługuje sytuacje wymagające działania użytkownika, jeśli jest to możliwe. Jeśli operacja nie może być kontynuowana bez działania użytkownika, zakończy się niepowodzeniem. Szczegółowe informacje na temat operacji, w tym błędy, które wystąpiły, można znaleźć w dzienniku operacji.

W przypadku wystąpienia błędu spróbuj ponownie

Ustawienie wstępne: **Włączone**. **Liczba ponawianych prób: 5. Odstęp między próbami: 30 sekund.**

Po wystąpieniu błędu, który można naprawić, program próbuje ponownie wykonać operację, która zakończyła się niepowodzeniem. Można ustawić odstęp pomiędzy kolejnymi próbami oraz ich liczbę. Ponowne próby zostaną wstrzymane po pomyślnym wykonaniu operacji LUB wykonaniu określonej liczby prób, w zależności od tego, który warunek zostanie spełniony wcześniej.

Jeśli na przykład lokalizacja sieciowa będzie niedostępna, program będzie próbował nawiązać połączenie co 30 sekund, ale nie więcej niż 5 razy. Próby zostaną zakończone po wznowieniu połączenia LUB wykonaniu określonej liczby prób, w zależności od tego, który warunek zostanie spełniony wcześniej.

Ustawienia dodatkowe

Określ dodatkowe ustawienia operacji odzyskiwania, zaznaczając lub czyszcząc poniższe pola wyboru.

Ustaw bieżącą datę i godzinę odzyskiwanych plików

Ta opcja jest dostępna tylko podczas odzyskiwania plików.

Ustawienie wstępne: **Włączone**.

Opcja określa, czy data i godzina plików mają być odzyskiwane z archiwum, czy też do plików ma być przypisywana bieżąca data i godzina.

Sprawdź poprawność kopii zapasowej przed odzyskiwaniem

Ustawienie wstępne: **Wyłączone**.

Opcja określa, czy przed odzyskaniem danych z kopii zapasowej należy sprawdzić jej poprawność. Dzięki temu można się upewnić, że kopia zapasowa nie jest uszkodzona.

Sprawdź system plików po odzyskaniu

Ta opcja jest dostępna tylko podczas odzyskiwania dysków lub woluminów.

Podczas pracy z nośnikiem startowym opcja jest niedostępna dla systemu plików NTFS.

Ustawienie wstępne: **Wyłączone**.

Opcja określa, czy po odzyskaniu dysku lub woluminu ma być sprawdzana integralność systemu plików.

Automatycznie ponownie uruchom komputer, gdy wymaga tego odzyskiwanie

Ta opcja jest dostępna, gdy odzyskiwanie odbywa się na komputerze z uruchomionym systemem operacyjnym.

Ustawienie wstępne: **Wyłączone**.

Opcja określa, czy komputer ma być automatycznie uruchamiany ponownie, gdy wymaga tego proces odzyskiwania. Może się tak zdarzyć w sytuacji, gdy trzeba odzyskać wolumin zablokowany przez system operacyjny.

Uruchom ponownie komputer po odzyskaniu

Ta opcja jest dostępna podczas pracy z nośnikiem startowym.

Ustawienie wstępne: **Wyłączone**.

Opcja umożliwia rozruch komputera w odzyskanym systemie operacyjnym bez działania użytkownika.

Zmień identyfikator SID po zakończeniu odzyskiwania

Ta opcja nie jest dostępna, gdy odzyskiwanie jest przeprowadzane na maszynę wirtualną przez komponent Acronis Backup & Recovery 10 Agent dla ESX/ESXi lub Acronis Backup & Recovery 10 Agent dla Hyper-V.

Ustawienie wstępne: **Wyłączone**.

Program Acronis Backup & Recovery 10 umożliwia wygenerowanie unikatowego identyfikatora zabezpieczeń (SID) dla odzyskanego systemu. W przypadku odzyskiwania systemu na nim samym lub tworzenia repliki systemu, która zastąpi oryginalny system, nowy identyfikator SID nie jest potrzebny. Należy go wygenerować, gdy system oryginalny i odzyskany będą pracowały jednocześnie w tej samej grupie roboczej lub domenie.

Użyj usługi FTP w trybie aktywnym

Ustawienie wstępne: **Wyłączone**.

Włącz tę opcję, jeśli serwer FTP obsługuje tryb aktywny i chcesz go używać do przesyłania plików.

Zarządzanie zasilaniem maszyn wirtualnych

Te opcje mają zastosowanie w przypadku maszyn wirtualnych znajdujących się na serwerach wirtualizacji.

Te opcje są dostępne tylko w przypadku, gdy na serwerze wirtualizacji jest zainstalowany agent maszyn wirtualnych Acronis.

Przed uruchomieniem odzyskiwania wyłącz docelowe maszyny wirtualne

Ustawienie wstępne: **Wł.**

Odzyskiwanie na istniejącej maszynie wirtualnej jest niemożliwe, gdy jest ona w trybie online, dlatego natychmiast po rozpoczęciu zadania odzyskiwania maszyna jest automatycznie wyłączana. Użytkownicy zostaną rozłączeni z maszyną, a wszelkie niezapisane dane zostaną utracone.

Jeśli użytkownik preferuje ręczne wyłączanie maszyn wirtualnych przed rozpoczęciem odzyskiwania, należy wyczyścić pole wyboru tej opcji.

Włącz docelową maszynę wirtualną po zakończeniu odzyskiwania

Ustawienie wstępne: **Wył.**

Po odzyskaniu maszyny z kopii zapasowej na innej maszynie może pojawić się w sieci replika istniejącej maszyny. Aby się przed tym zabezpieczyć, należy ręcznie włączyć maszynę wirtualną, podejmując uprzednio niezbędne środki ostrożności.

Jeśli jest wymagane automatyczne włączanie maszyny wirtualnej, należy zaznaczyć pole wyboru tej opcji.

4 Skarbce

Skarbiec to lokalizacja do zachowywania archiwów kopii zapasowych. W celu ułatwienia obsługi i administracji skarbiec jest powiązany z metadanymi archiwów. Odwoływanie do takich metadanych przyspiesza operacje na archiwach i kopiach zapasowych przechowywanych w skarbcu i sprawia, ich wykonywanie jest wygodniejsze.

Skarbiec można zorganizować na dysku lokalnym lub sieciowym, nośniku odłączanym lub urządzeniu taśmowym dołączonym do węzła Acronis Backup & Recovery 10 Storage Node.

Nie istnieją żadne ustawienia do ograniczania rozmiaru skarbca ani liczby kopii zapasowych w skarbcu. Rozmiar każdego archiwum można ograniczyć przy użyciu funkcji czyszczenia, ale łączny rozmiar archiwów przechowywanych w skarbcu jest ograniczony tylko rozmiarem samego skarbca.

Po co tworzyć skarbce?

Zaleca się utworzenie skarbca w każdym miejscu docelowym, w którym mają być przechowywane archiwa kopii zapasowych. Ułatwi to pracę w następujący sposób.

Szybki dostęp do skarbca

Nie trzeba będzie pamiętać ścieżek do folderów, w których są przechowywane archiwa. Przy tworzeniu planu tworzenia kopii zapasowych albo zadania wymagającego wyboru archiwum lub miejsca docelowego archiwum będzie dostępna lista skarbców, która zapewni szybki dostęp do skarbca bez konieczności rozwijania drzewa folderów.

Łatwe zarządzanie archiwami

Skarbiec jest dostępny z panelu **Nawigacja**. Zaznaczając skarbiec, można przejrzeć archiwa w nim przechowywane oraz wykonać następujące operacje zarządzania archiwum:

- pobranie listy kopii zapasowych znajdujących się w każdym archiwum:
- odzyskanie danych z kopii zapasowej,
- sprawdzenie zawartości kopii zapasowej,
- sprawdzenie poprawności wszystkich archiwów w skarbcu lub poszczególnych archiwach i kopiach zapasowych,
- zamontowanie kopii zapasowej woluminu w celu skopiowania plików z kopii zapasowej na dysk fizyczny,
- bezpieczne usunięcie archiwów oraz kopii zapasowych z archiwów.

Tworzenie skarbców jest bardzo zalecane, ale nie jest obowiązkowe. Można nie korzystać ze skrótów i zawsze określać pełną ścieżkę do skarbca archiwów. Wszystkie operacje powyżej, z wyjątkiem usunięcia archiwum i kopii zapasowej, można wykonać bez tworzenia skarbców.

W wyniku operacji utworzenia skarbca jego nazwa zostanie dodana w sekcji **Skarbce** na panelu **Nawigacja**.

Skarbce centralne i osobiste

Skarbiec centralny to lokalizacja sieciowa przydzielona przez administratora serwera zarządzania służąca jako magazyn archiwów kopii zapasowych. Skarbiec centralny może być zarządzany przy użyciu węzła magazynowania (skarbiec zarządzany) lub niezarządzany.

Skarbiec osobisty to skarbiec utworzony przy użyciu bezpośredniego połączenia konsoli z komputerem zarządzanym. Skarbce osobiste są specyficzne dla każdego komputera zarządzanego.

Sposób pracy z widokiem „Skarbce”

Skarbce (na panelu nawigacji) — początkowy element drzewa skarbców. Kliknij go, aby wyświetlić grupy skarbców centralnych i osobistych.

Centralne. Jest to grupa dostępna po połączeniu konsoli z komputerem zarządzanym lub serwerem zarządzania. Rozwiń ją, aby wyświetlić listę skarbców centralnych dodanych przez administratora serwera zarządzania.

Kliknij dowolny skarbiec centralny w drzewie, aby otworzyć szczegółowy widok tego skarbca (s. 146) i wykonać czynności w samym skarbcu (s. 147) oraz archiwach (s. 181) i kopiach zapasowych (s. 182) w nim przechowywanych.

Osobiste. Jest to grupa dostępna po połączeniu konsoli z komputerem zarządzanym. Rozwiń tę grupę, aby wyświetlić listę skarbców osobistych utworzonych na komputerze zarządzanym.

Kliknij dowolny skarbiec osobisty w drzewie, aby otworzyć szczegółowy widok tego skarbca (s. 178) i wykonać czynności w samym skarbcu (s. 179) oraz archiwach (s. 181) i kopiach zapasowych (s. 182) w nim przechowywanych.

4.1 Skarbce centralne

Skarbiec centralny to lokalizacja sieciowa wyznaczona przez administratora serwera zarządzania do przechowywania archiwów kopii zapasowych. Skarbiec centralny może być zarządzany przy użyciu węzła magazynowania albo niezarządzany. Łączna liczba archiwów przechowywanych w skarbcu centralnym i ich rozmiar są ograniczone wyłącznie rozmiarem magazynu.

Niezwłocznie po utworzeniu skarbca centralnego przez administratora serwera zarządzania nazwa i ścieżka tego skarbca są dystrybuowane na wszystkie komputery zarejestrowane na serwerze. W grupie **Skarbce > Centralne** na komputerach pojawi się skrót do skarbca. Ze skarbca centralnego można korzystać we wszelkich planach tworzenia kopii zapasowych istniejących na komputerach, w tym również planach lokalnych.

Na komputerze, który nie jest zarejestrowany na serwerze zarządzania, użytkownik mający uprawnienia do tworzenia kopii zapasowej w skarbcu centralnym może wykonać tę czynność, określając pełną ścieżkę do skarbca. Jeśli skarbiec jest zarządzany, zarówno archiwa użytkownika, jak i inne archiwa przechowywane w skarbcu, będą zarządzane przy użyciu węzła magazynowania.

Skarbce zarządzane

Skarbiec zarządzany to skarbiec centralny zarządzany przez węzeł magazynowania.

Węzeł magazynowania wykonuje zadania czyszczenia (s. 420) oraz sprawdzania poprawności (s. 429) w odniesieniu do każdego archiwum przechowywanego w skarbcu zarządzanym, tak jak to określono w planach tworzenia kopii zapasowych (s. 425). Podczas tworzenia skarbca zarządzanego administrator może określić dodatkowe operacje, które wykona węzeł magazynowania: deduplikację i szyfrowanie. Aby uzyskać więcej informacji, zobacz „Operacje wykonywane przez węzły magazynowania”.

Każdy skarbiec zarządzany jest samowystarczalny, co oznacza, że zawiera wszystkie metadane potrzebne do zarządzania nim przez węzeł magazynowania. Skarbiec można dołączyć do innego węzła magazynowania. Nowy węzeł magazynowania pobierze metadane ze skarbca i ponownie utworzy bazę danych konieczną do zarządzania skarbcem. Aby uzyskać więcej informacji, zobacz „Dołączanie skarbca zarządzanego” (s. 152).

Dostęp do skarbców zarządzanych

Użytkownicy muszą mieć uprawnienia administratora lub użytkownika, aby uzyskać dostęp do skarbca. Administratorzy serwera zarządzania domyślnie uzyskują uprawnienia administratora. Uprawnienia dla innych użytkowników można określić podczas tworzenia lub edycji skarbca. Aby uzyskać więcej informacji, zobacz „Uprawnienia użytkownika w węźle magazynowania” (s. 90).

Skarbce niezarządzane

Skarbiec niezarządzany to skarbiec centralny, który nie jest zarządzany przy użyciu węzła magazynowania. Aby uzyskać dostęp do skarbca niezarządzanego, należy mieć uprawnienia dostępu do lokalizacji z sieci.

Wszyscy użytkownicy mający uprawnienia odczytu/zapisu plików w skarbcu niezarządzanym mogą:

- tworzyć kopię zapasową danych w skarbcu niezarządzanym,
- odzyskiwać dane z dowolnej kopii zapasowej znajdującej się w skarbcu niezarządzanym,
- przeglądać i zarządzać wszystkimi archiwami w skarbcu niezarządzanym.

4.1.1 Praca z widokiem „Skarbiec centralny”

W tej sekcji krótko opisano główne elementy widoku **Skarbiec centralny** oraz przedstawiono sugestie dotyczące sposobu pracy z nim.

Pasek narzędzi skarbca

Pasek narzędzi zawiera przyciski operacyjne umożliwiające wykonanie operacji na wybranym skarbcu centralnym. Aby uzyskać szczegółowe informacje na ten temat, zobacz sekcję Czynności dotyczące skarbców centralnych (s. 147).

Wykres kołowy z legendą

Wykres kołowy umożliwia oszacowanie obciążenia skarbca. Przedstawia stosunek wolnego do zajętego miejsca w skarbcu. Wykres kołowy jest niedostępny, gdy skarbiec znajduje się w bibliotece taśmowej.

— wolne miejsce: miejsce w urządzeniu pamięci, w którym znajduje się skarbiec. Jeśli na przykład skarbiec znajduje się na dysku twardym, wolnym miejscem skarbca jest wolne miejsce odpowiedniego woluminu.

— zajęte miejsce: łączny rozmiar archiwów kopii zapasowych i ich metadanych, o ile znajdują się w skarbcu.

Legenda zawiera następujące informacje o skarbcu:

- [tylko skarbce zarządzane] nazwa węzła magazynowania zarządzającego skarbcem;
- pełna ścieżka do skarbca;
- łączna liczba archiwów i kopii zapasowych przechowywanych w skarbcu;
- współczynnik zajętego miejsca do rozmiaru oryginalnych danych;
- [tylko skarbce zarządzane] stan deduplikacji (s. 81) (włączona lub wyłączona);
- [tylko skarbce zarządzane] stan szyfrowania (tak lub nie).

Zawartość skarbca

W sekcji **Zawartość skarbca** znajdują się tabela i pasek narzędzi archiwów. Tabela archiwów zawiera archiwa i kopie zapasowe przechowywane w skarbcu. Pasek narzędzi archiwów służy do wykonywania czynności na wybranych archiwach i kopiach zapasowych. Lista kopii zapasowych rozwija się po kliknięciu znaku „plus” z lewej strony nazwy archiwum. Wszystkie archiwa są pogrupowane według typów na następujących kartach:

- Na karcie **Archiwa dyskowe** znajduje się lista wszystkich archiwów zawierających kopie zapasowe (obrazy) dysków lub woluminów.
- Na karcie **Archiwa plikowe** znajduje się lista wszystkich archiwów zawierających kopie zapasowe plików.

Sekcje pokrewne:

Operacje na archiwach przechowywanych w skarbcu (s. 181)

Operacje na kopiach zapasowych (s. 182)

Filtrowanie i sortowanie archiwów (s. 183)

Paski na panelu „Czynności i narzędzia”

- **[Nazwa skarbca]** Pasek **Czynności** jest dostępny po kliknięciu skarbca w drzewie skarbców. Umożliwia wykonanie tych samych czynności, co pasek narzędzi skarbca.
- **[Nazwa archiwum]** Pasek **Czynności** jest dostępny po wybraniu archiwum w tabeli archiwów. Umożliwia wykonanie tych samych czynności, co pasek narzędzi archiwów.
- **[Nazwa kopii zapasowej]** Pasek **Czynności** jest dostępny po rozwinięciu archiwum i kliknięciu dowolnej z jego kopii zapasowych. Umożliwia wykonanie tych samych czynności, co pasek narzędzi archiwów.

4.1.2 Czynności dotyczące skarbców centralnych

Wszystkie opisane tutaj operacje wykonuje się przez kliknięcie odpowiednich przycisków na pasku narzędzi skarbców. Dostęp do tych operacji można również uzyskać na pasku **Czynności [nazwa skarbca]** (w panelu **Czynności i narzędzia**) oraz za pomocą elementu **Czynności [nazwa skarbca]** w menu głównym.

Poniżej przedstawiono wskazówki dotyczące wykonywania operacji na skarbcach centralnych.

Zadanie	Czynności
Tworzenie skarbca zarządzanego lub niezarządzanego	1. Kliknij **Utwórz**. 2. W polu **Typ** wybierz typ skarbca: **Zarządzany** lub **Niezarządzany** Procedurę tworzenia skarbców centralnych opisano szczegółowo w następujących sekcjach: ▪ Tworzenie zarządzanego skarbca centralnego (s. 149) ▪ Tworzenie niezarządzanego skarbca centralnego (s. 151)
Edytowanie skarbca zarządzanego lub niezarządzanego	1. Wybierz skarbiec. 2. Kliknij **Edytuj**. W zależności od wybranego skarbca (zarządzanego lub

	niezarządzanego) zostanie otwarta odpowiednia strona edycji: ▪ Na stronie **Edytuj skarbiec zarządzany** można zmienić nazwę skarbca, hasło szyfrowania (jeśli skarbiec jest zaszyfrowany) i informacje w polu **Komentarze**. ▪ Na stronie **Edytuj skarbiec niezarządzany** można zmienić nazwę skarbca i informacje w polu **Komentarze**.
Sprawdzanie poprawności skarbca	1. Wybierz skarbiec. 2. Kliknij **Sprawdź poprawność**. Nastąpi przejście do strony Sprawdzanie poprawności (s. 271) ze wstępnie wybranym skarbcem jako źródłem. Sprawdzenie poprawności skarbca polega na sprawdzeniu wszystkich archiwów w tym skarbcu.
Usuwanie skarbca	1. Wybierz skarbiec. 2. Kliknij **Usuń**. Pojawi się pytanie, czy chcesz zachować archiwa zawarte w skarbcu, czy usunąć skarbiec razem z wszystkimi archiwami. Wykonanie planów i zadań wymagających użycia tego skarbca zakończy się niepowodzeniem. Jeśli zdecydujesz się zachować archiwa skarbca zarządzanego, skarbiec zostanie odłączony od węzła magazynowania. Później skarbiec będzie można dołączyć do tego samego lub innego węzła magazynowania.
Eksplorowanie skarbca niezarządzanego	1. Wybierz skarbiec niezarządzany. 2. Kliknij **Eksploruj**. Skarbiec będzie można przeglądać przy użyciu zwykłego menedżera plików.
Dołączanie skarbca zarządzanego, który został usunięty bez usuwania zawartości	Kliknij **Dołącz**. Procedurę dołączania skarbca zarządzanego do węzła magazynowania opisano szczegółowo w sekcji Dołączanie skarbca zarządzanego (s. 152).
Zmiana poświadczeń użytkownika umożliwiających dostęp do skarbca	Kliknij **Zmień użytkownika**. Poświadczenia użytkownika można zmienić tylko w przypadku skarbców znajdujących się w magazynach udostępnionych.
Odświeżanie informacji o skarbcu	Kliknij **Odśwież**. Podczas przeglądania zawartości skarbca można dodawać, usuwać i modyfikować jego archiwa. Kliknij **Odśwież**, aby w informacjach dotyczących skarbca uwzględnić najnowsze zmiany.
Czynności dotyczące biblioteki taśm w skarbcu zarządzanym	
Definiowanie etykiet taśm i wykonywanie inwentaryzacji biblioteki taśm w skarbcu zarządzanym	Kliknij **Zarządzaj taśmami**. W oknie **Zarządzanie taśmami** zdefiniuj etykiety taśm i odśwież spis. Aby uzyskać więcej informacji, zobacz sekcję Zarządzanie biblioteką taśm (s. 159).
Ponowne skanowanie taśm w skarbcach zarządzanych	Kliknij **Skanuj ponownie taśmy**. Ponowne skanowanie polega na odczytaniu informacji na temat zawartości taśm wybranych przez użytkownika i zaktualizowaniu bazy danych węzła magazynowania.

	Ta operacja jest opisana szczegółowo w sekcji Ponowne skanowanie (s. 159).

Tworzenie zarządzanego skarbca centralnego

Aby utworzyć zarządzany skarbiec centralny, wykonaj następujące kroki

Skarbiec

Nazwa

Określ unikatową nazwę skarbca. Utworzenie dwóch skarbców centralnych o tej samej nazwie jest zabronione.

Komentarze

[Opcjonalnie] Wprowadź charakterystyczny opis tworzonego skarbca.

Typ

Wybierz typ **Zarządzany**.

Węzeł magazynowania

Wybierz węzeł Acronis Backup & Recovery 10 Storage Node, który będzie zarządzać skarbcem. Może być konieczne wprowadzenie poświadczeń dostępu do węzła magazynowania.

Ścieżka (s. 150)

Określ lokalizację, w której zostanie utworzony skarbiec. Zarządzane skarbce centralne mogą znajdować się w udziale sieciowym, SAN, NAS lub na lokalnym dysku twardym węzła magazynowania.

Ścieżka bazy danych (s. 150)

Określ folder lokalny na serwerze pamięci masowej, aby utworzyć bazę danych skarbca. W tej bazie danych będą przechowywane metadane wymagane do katalogowania archiwów i wykonywania deduplikacji.

Deduplikacja

[Opcjonalnie] Zdecyduj, czy ma być włączona deduplikacja archiwów w skarbcu. Deduplikacja zmniejsza ilość miejsca zajmowaną przez archiwa oraz ruch sieciowy przy tworzeniu kopii zapasowej. Funkcja ogranicza rozmiar archiwów w skarbcu, eliminując nadmiarowe dane, takie jak zduplikowane pliki i bloki danych.

Deduplikacja nie jest możliwa na urządzeniach taśmowych.

Aby dowiedzieć się więcej, na czym polega deduplikacja, zobacz sekcję Deduplikacja (s. 81).

Kompresja

[Opcjonalnie] Zdecyduj, czy magazyn danych deduplikacji ma być kompresowany. To ustawienie jest dostępne tylko po włączeniu deduplikacji.

Szyfrowanie (s. 150)

[Opcjonalnie] Zdecyduj, czy skarbiec ma być chroniony przez szyfrowanie. Wszelkie informacje zapisywane w skarbcu będą szyfrowane, a wszelkie informacje odczytywane z niego będą odszyfrowywane w czasie rzeczywistym przez węzeł magazynowania przy użyciu klucza szyfrowania specyficznego dla skarbca i przechowywanego w tym węźle.

Po wykonaniu wszystkich wymaganych kroków kliknij **OK**, aby utworzyć skarbiec zarządzany.

Ścieżka skarbca

Aby określić ścieżkę, w której zostanie utworzony skarbiec zarządzany

1. Wprowadź pełną ścieżkę do folderu w polu **Ścieżka** lub wybierz żądany folder w drzewie folderów. Skarbce zarządzane można zorganizować:
   - na lokalnych dyskach twardych węzła magazynowania;
   - w udziale sieciowym;
   - w sieci SAN (Storage Area Network);
   - w magazynie NAS (Network Attached Storage);
   - w bibliotece taśmowej dołączonej lokalnie do węzła magazynowania.

   Aby utworzyć nowy folder skarbca w wybranej lokalizacji, kliknij **Utwórz folder**.
2. Kliknij **OK**.

Skarbiec można utworzyć wyłącznie w pustym folderze.

Nie zaleca się tworzenia skarbca zarządzanego w woluminie FAT32 i deduplikowanie *go, ponieważ w takich skarbcach wszystkie zdeduplikowane elementy znajdują się w dwóch potencjalnie dużych plikach. Maksymalny rozmiar pliku w systemach plików FAT to 4 GB, dlatego po przekroczeniu tego limitu węzeł magazynowania może przestać działać.*

Ścieżka bazy danych skarbca

Aby określić ścieżkę, w której zostanie utworzona baza danych skarbca

1. W grupie **Foldery lokalne** węzła magazynowania wybierz żądany folder lub wprowadź jego pełną ścieżkę w polu **Ścieżka**.

   Aby utworzyć nowy folder bazy danych, kliknij **Utwórz folder**.
2. Kliknij **OK**.

Podczas wybierania folderu dla bazy danych skarbca należy wziąć pod uwagę następujące czynniki:

- Folder musi znajdować się na stałym dysku. Nie należy umieszczać bazy danych na zewnętrznych dyskach wymiennych.
- Folder może osiągnąć bardzo duże rozmiary — szacunkowo około 200 GB na 8 TB użytego miejsca, czyli około 2,5 procenta.
- Uprawnienia folderu muszą umożliwiać zapisywanie w folderze przy użyciu konta użytkownika, którego użyto do uruchomienia usługi węzła magazynowania (domyślnie: **Użytkownik ASN**). Podczas przypisywania uprawnień należy wprost określić konto użytkownika (nie tylko: **Wszyscy**).

Szyfrowanie skarbca

Jeśli skarbiec jest chroniony za pomocą szyfrowania, wszystkie dane zapisywane w skarbcu są szyfrowane, a wszystkie odczytywane dane są deszyfrowane w przezroczysty sposób przez węzeł magazynowania przy użyciu klucza szyfrowania skarbca przechowywanego w tym węźle. W przypadku kradzieży nośnika danych lub uzyskania do niego dostępu przez osobę nieuprawnioną odszyfrowanie zawartości skarbca bez dostępu do węzła magazynowania będzie niemożliwe.

To szyfrowanie nie ma nic wspólnego z szyfrowaniem archiwum określonym w planie tworzenia kopii zapasowych i wykonywanym przez agenta. Jeśli archiwum jest już zaszyfrowane, szyfrowanie po stronie węzła magazynowania zostanie zastosowane po szyfrowaniu wykonanym przez agenta.

Aby ustawić ochronę skarbca za pomocą szyfrowania

1. Zaznacz pole wyboru **Szyfruj**.
2. W polu **Wprowadź hasło** wpisz hasło.
3. W polu **Potwierdź hasło** wpisz ponownie hasło.
4. Wybierz jedną z następujących opcji:
   - **AES 128** — zawartość skarbca będzie szyfrowana przy użyciu algorytmu Advanced Encryption Standard (AES) z kluczem 128-bitowym.
   - **AES 192** — zawartość skarbca będzie szyfrowana przy użyciu algorytmu AES z kluczem 192-bitowym.
   - **AES 256** — zawartość skarbca będzie szyfrowana przy użyciu algorytmu AES z kluczem 256-bitowym.
5. Kliknij **OK**.

Algorytm kryptograficzny AES działa w trybie wiązania bloków szyfrogramu (Cipher-Block Chaining — CBC) i korzysta z losowo wygenerowanego klucza o długości zdefiniowanej przez użytkownika: 128, 192 lub 256 bitów. Im większy rozmiar klucza, tym dłużej trwa szyfrowanie archiwów przechowywanych w skarbcu, ale są one lepiej zabezpieczone.

Klucz szyfrowania jest następnie szyfrowany metodą AES-256, w której jako klucz służy skrót SHA-256 hasła. Samo hasło nie jest przechowywane w żadnym miejscu na dysku — do celów weryfikacji służy skrót hasła. Dzięki tym dwupoziomowym zabezpieczeniom archiwa są chronione przed nieautoryzowanym dostępem, ale odzyskanie utraconego hasła jest niemożliwe.

Tworzenie niezarządzanego skarbca centralnego

Aby utworzyć niezarządzany skarbiec centralny, wykonaj następujące kroki.

Skarbiec

Nazwa

Określ unikatową nazwę skarbca. Utworzenie dwóch skarbców centralnych o tej samej nazwie jest zabronione.

Komentarze

Wprowadź charakterystyczny opis skarbca.

Typ

Wybierz typ **Niezarządzany**.

Ścieżka (s. 151)

Określ lokalizację, w której zostanie utworzony skarbiec.

Po wykonaniu wszystkich wymaganych kroków kliknij **OK**, aby utworzyć niezarządzany skarbiec centralny.

Ścieżka skarbca

Aby określić ścieżkę, w której zostanie utworzony skarbiec niezarządzany

1. Wprowadź pełną ścieżkę do folderu w polu Ścieżka lub wybierz odpowiedni folder w drzewie folderów. Skarbce niezarządzane można zakładać:
   - Magazyn Acronis Online Backup Storage
   - w udziale sieciowym,
   - w sieci SAN (Storage Area Network),

- w magazynie NAS (Network Attached Storage),
- na serwerze FTP lub SFTP.

Jak wynika z oryginalnej specyfikacji protokołu FTP, poświadczenia wymagane do uzyskania dostępu do serwerów FTP są przesyłane w sieci jako otwarty tekst. Oznacza to, że nazwę użytkownika i hasło można przejąć przy użyciu programu do przechwytywania pakietów.

Aby utworzyć nowy folder dla skarbca, kliknij  Utwórz folder.

Skarbiec można utworzyć wyłącznie w pustym folderze.

2. Kliknij OK.

Dołączanie skarbca zarządzanego

Skarbiec zarządzany przy użyciu węzła magazynowania można dołączyć do innego węzła magazynowania. Może to być konieczne przy odłączaniu sprzętu węzła magazynowania, po utracie tego węzła lub w celu zrównoważenia obciążenia między węzłami. W efekcie pierwszy węzeł przestanie zarządzać skarbcem. Drugi węzeł przeskanuje archiwa w skarbcu, utworzy bazę danych i wypełni ją odpowiednimi danymi skarbca i rozpocznie zarządzanie tym skarbcem.

Usuwając skarbiec zarządzany, można pozostawić archiwa znajdujące się w skarbcu. Lokalizację powstałą po takiej operacji usunięcia można również dołączyć do tego samego lub innego węzła magazynowania.

Nie można dołączać niezarządzanych skarbców osobistych ani centralnych.

Aby dołączyć skarbiec zarządzany do węzła magazynowania, wykonaj następujące kroki.

Skarbiec

Węzeł magazynowania

Wybierz węzeł magazynowania Acronis Backup & Recovery 10 Storage Node, który będzie zarządzać skarbcem.

Ścieżka

Określ ścieżkę do lokalizacji, w której są przechowywane archiwa.

Ścieżka bazy danych

Określ folder lokalny na serwerze pamięci masowej, aby utworzyć bazę danych skarbca. W tej bazie danych będą przechowywane metadane wymagane do katalogowania archiwów i wykonywania deduplikacji.

Hasło

Jeśli skarbiec został zaszyfrowany, należy wprowadzić hasło szyfrowania.

Po wykonaniu wszystkich wymaganych kroków kliknij **OK**, aby dołączyć skarbiec. Procedura może zająć dłuższą chwilę, ponieważ węzeł magazynowania musi przeskanować archiwa, zapisać metadane w bazie danych oraz zdeduplikować archiwa, jeśli oryginalnie był to skarbiec deduplikacji.

4.1.3 Biblioteki taśm

W tej sekcji szczegółowo opisano sposób używania automatycznych urządzeń taśmowych jako skarbców, w których są zapisywane archiwa kopii zapasowych.

Biblioteka taśm (biblioteka automatyczna) to urządzenie pamięci o dużej pojemności składające się z następujących elementów:

- jednego lub kilku napędów taśm;

- wielu (nawet do kilku tysięcy) gniazd do przechowywania kaset z taśmami;
- jednego lub kilku urządzeń ładujących (automatów), których zadaniem jest przenoszenie kaset z taśmami pomiędzy gniazdami a napędami taśm;
- czytników kodów kreskowych (opcjonalnie).

Omówienie

Program Acronis Backup & Recovery 10 w pełni obsługuje biblioteki taśm przy użyciu węzła magazynowania Acronis Backup & Recovery 10 Storage Node. Węzeł magazynowania należy zainstalować na komputerze, do którego jest podłączona biblioteka taśm. Węzeł magazynowania może jednocześnie używać kilku bibliotek taśm do przechowywania archiwów.

Do zarządzania nośnikiem biblioteki taśm węzeł magazynowania używa systemu Windows Removable Storage Manager (RSM). Więcej informacji na ten temat można znaleźć w sekcji Pule nośników RSM (s. 154).

Informacje na temat zawartości kopii zapasowej zapisanej na taśmach znajdują się w dedykowanej bazie danych węzła magazynowania. Dlatego niektóre operacje (na przykład Czyszczenie (s. 419)) można wykonać szybko, bez uzyskiwania dostępu do nośnika. Można przeglądać zawartość archiwum kopii zapasowej przy użyciu konsoli, nawet gdy biblioteka taśm jest wyłączona, ponieważ informacje są zapisane w bazie danych. W celu utworzenia przyrostowej lub różnicowej kopii zapasowej program używa bazy danych zamiast ładowania, montowania, przewijania i odczytywania taśmy zawierającej pełną kopię zapasową. Jednak odczytanie taśmy jest niezbędne podczas operacji, takich jak sprawdzanie poprawności (s. 429) kopii zapasowej lub odzyskiwanie danych.

Do komputera, na którym jest zainstalowany agent, można podłączyć bibliotekę taśm tylko wtedy, gdy biblioteka będzie traktowana jako napęd z jedną taśmą. Agent może używać takiego urządzenia do zapisywania i odczytywania kopii zapasowych danych, ale format kopii zapasowych różni się od formatu kopii zapasowych na taśmach zapisywanych przez węzeł magazynowania. Więcej informacji na temat możliwości odczytania przez program Acronis Backup & Recovery 10 archiwów zapisanych na taśmach przy użyciu różnych komponentów lub wersji produktu można znaleźć w sekcji Tabela kompatybilności taśm (s. 57).

Program Acronis Backup & Recovery 10 umożliwia ustawianie dystrybucji kopii zapasowych według nośników. Można na przykład użyć oddzielnego zestawu taśm do utworzenia kopii zapasowej określonych danych, a kopie pozostałych danych program zapisze na aktualnie zamontowanej taśmie, która nie należy do zestawu. Więcej informacji na ten temat można znaleźć w sekcji Obsługa taśmy (s. 130).

Schematy tworzenia kopii zapasowych (Dziadek-ojciec-syn (s. 38), Wieża Hanoi (s. 42)) znacząco ułatwiają utworzenie efektywnego harmonogramu i reguł przechowywania kopii zapasowych w bibliotece taśm. Wraz z opcjami taśm schematy tworzenia kopii zapasowych umożliwiają ponowne wykorzystanie w trybie automatycznym taśm, które są uważane za puste po usunięciu z nich kopii zapasowych. Więcej informacji na ten temat można znaleźć w sekcji Rotacja taśm (s. 162).

Sprzęt

Biblioteka taśm (biblioteka automatyczna) to urządzenie pamięci o dużej pojemności składające się z następujących elementów:

- jednego lub kilku napędów taśm;
- wielu (nawet do kilku tysięcy) gniazd do przechowywania kaset z taśmami;
- jednego lub kilku urządzeń ładujących (automatów), których zadaniem jest przenoszenie kaset z taśmami pomiędzy gniazdami a napędami taśm;

- czytników kodów kreskowych (opcjonalnie).

Każda taśma może mieć z boku kasety naklejoną specjalną etykietę składającą się z:

- kodu kreskowego skanowanego przez specjalny czytnik zamontowany zwykle w urządzeniu ładującym;
- czytelnej wartości liczbowej kodu kreskowego.

Etykiety te są używane do identyfikacji taśm w bibliotece taśm, zwłaszcza w magazynach znajdujących się w innej lokalizacji.

Jeśli wszystkie kasety w bibliotece taśm mają kody kreskowe, oprogramowanie może nią zarządzać automatycznie.

Biblioteki taśm są ekonomicznym rozwiązaniem w magazynach danych o bardzo dużej pojemności. Taśmy są idealne do archiwizacji również ze względu na możliwość ich przechowywania w innej lokalizacji w celu zwiększenia bezpieczeństwa danych. Jednak odczytanie nawet niewielkiej ilości danych z biblioteki taśm zajmuje dużo więcej czasu (od kilku sekund do kilku minut) niż w przypadku innych typów magazynów danych. Najlepszym sposobem używania taśm jest „MNIEJ żądań odczytu/zapisu DUŻEJ ilości danych". Zatem dla biblioteki taśm bardziej odpowiednim podejściem jest systematyczne uzyskiwanie dostępu do dużych ilości danych a nie losowy dostęp do małych ilości danych.

Ograniczenia

Istnieją następujące ograniczenia w wykorzystaniu biblioteki taśm:

1. Dla archiwów zapisanych na taśmach nie można wykonać operacji konsolidacji (s. 424). Nie można usunąć z taśmy pojedynczej, oddzielnej kopii zapasowej. Można usunąć wszystkie kopie zapasowe zapisane na taśmie. Jednak po wykonaniu tej operacji nie będzie można odzyskać danych z wszystkich przyrostowych i różnicowych kopii zapasowych zapisanych na innych taśmach, których podstawę stanowiły usunięte kopie zapasowe. Dla reguł przechowywania planu tworzenia kopii zapasowych **Niestandardowe** opcja **Jeśli usunięcie kopii zapasowej ma wpływ na inne kopie zapasowe > Konsoliduj kopie zapasowe** jest niedostępna. Dostępna jest tylko opcja **Wstrzymaj usunięcie**.
2. Deduplikacja (s. 420) jest niedostępna dla archiwów zapisanych na urządzeniach taśmowych.
3. Z kopii zapasowej dysku zapisanej na taśmie można odzyskiwać pliki, ale może to zająć bardzo dużo czasu.
4. Nie można odczytać taśmy zawierającej kopie zapasowe zapisane przez węzeł magazynowania w urządzeniu taśmowym podłączonym lokalnie do komputera, na którym jest zainstalowany agent, ponieważ format zapisania taśmy jest inny. Informacje na temat możliwości odczytania archiwów zapisanych na taśmach przez różne komponenty innych wersji produktu za pomocą programu Acronis Backup & Recovery 10 można znaleźć w sekcji Tabela kompatybilności taśm (s. 57).
5. Drukarki kodów kreskowych nie są używane.

Pule nośników RSM

Do zarządzania kasetami taśm należącymi do poszczególnych bibliotek taśm program Acronis Backup & Recovery 10 używa systemu Windows Removable Storage Manager (RSM).

W celu określenia możliwości dostępu do nośnika przez różne programy system RSM używa pul nośników, które są logicznymi grupami nośników. W menedżerze istnieją dwie kategorie pul nośników: **System** i **Aplikacja**.

Do pul nośników **System** należą pule **Wolny**, **Import** i **Nierozpoznany**. W pulach **System** znajdują się nośniki, które nie są aktualnie używane przez aplikacje. W puli **Wolny** znajdują się nośniki uważane za

wolne, które mogą być używane przez aplikacje. **Import** i **Nierozpoznany** to pule tymczasowe dla nowych nośników w danej bibliotece.

Przy użyciu systemu RSM aplikacja może uzyskać własne pule z odpowiednimi nazwami, przenosić nośniki z puli **Wolny** do własnych pul, używać własnych pul nośników do odpowiednich celów, zwracać nośniki do puli **Wolny** itp.

Węzeł magazynowania Acronis Backup & Recovery 10 Storage Node zarządza taśmami należącymi do puli **Acronis**.

Po włożeniu nieużywanych taśm do gniazd biblioteki taśm program automatycznie dołączy wszystkie taśmy do puli **Wolny**.

Jeśli taśma była wcześniej używana, system RSM spróbuje wykryć zarejestrowaną aplikację, z którą jest związana taśma. Jeśli system RSM nie znajdzie aplikacji, przeniesie taśmę do puli **Nierozpoznany**. Jeśli system RSM nie znajdzie aplikacji, ale w jego bazie danych nie ma informacji na temat taśmy, przeniesie taśmę do puli **Import**. Jeśli w bazie danych systemu RSM znajdują się odpowiednie informacje, system przeniesie taśmę do puli odpowiedniej aplikacji.

Węzeł magazynowania Acronis Backup & Recovery 10 Storage Node umożliwia systemowi RSM wykrywanie taśm zapisanych przez produkty z rodzin Acronis True Image Echo, Acronis True Image 9.1 oraz komponenty produktu Acronis Backup & Recovery 10. Węzeł magazynowania umieszcza wszystkie taśmy zapisane w formacie „Acronis" w puli **Acronis** podczas wykonywania operacji Inwentaryzacja (s. 159).

Komponenty produktu Acronis Backup & Recovery 10 nie używają puli **Nierozpoznany**. Aby wymusić użycie taśmy z tej puli, należy przenieść taśmę do puli **Wolny** przy użyciu dodatku magazynu wymiennego (**Panel sterowania > Narzędzia administracyjne > Zarządzanie komputerem > Magazyn wymienny > Pule nośników**).

*Po przeniesieniu taśmy do puli **Wolny** jest ona uważana za wolną i będzie dostępna do zapisu dla wszystkich aplikacji. Dane na taśmie zostaną zatem utracone.*

Po usunięciu wszystkich kopii zapasowych z taśmy program nie przeniesie jej do puli **Wolny**. Pozostanie ona w puli **Acronis** jako wolna taśma gotowa do ponownego użycia. Zatem gdy węzeł magazynowania będzie wymagał nowej taśmy, znajdzie ją najpierw w puli **Acronis**, a dopiero potem w puli **Wolny**.

Dlatego węzeł magazynowania Acronis Backup & Recovery 10 Storage Node obsługuje tylko taśmy należące do puli **Acronis**.

Rozpoczęcie pracy z biblioteką taśm

Jeśli do komputera, na którym jest zainstalowany węzeł magazynowania Acronis Backup & Recovery 10 Storage Node, jest podłączone urządzenie biblioteki taśm, w celu utworzenia kopii zapasowej w bibliotece taśm wystarczy utworzyć na urządzeniu skarbiec archiwów zarządzany przez węzeł magazynowania.

Wymagania wstępne

Urządzenie biblioteki taśm należy zainstalować na komputerze z systemem Windows zgodnie z instrukcją instalacji dostarczoną przez producenta urządzenia.

Jeśli w używanej wersji systemu Windows jest dostępny system Removable Storage Manager (RSM), należy go aktywować.

W systemie Microsoft Windows XP i Microsoft Windows Server 2003:

- System Removable Storage Manager jest częścią systemu operacyjnego i jest aktywowany po uruchomieniu systemu.

Aby aktywować system Removable Storage Manager w systemie Microsoft Windows Server 2008:

1. Kliknij **Narzędzia administracyjne > Menedżer serwerów > Funkcje > Dodaj funkcję**.
2. Zaznacz pole wyboru **Menedżer magazynu wymiennego**.

Aby aktywować system Removable Storage Manager w systemie Microsoft Windows Vista:

1. Kliknij **Panel sterowania > Programy > Programy i funkcje > Włącz lub wyłącz funkcje systemu Windows**.
2. Zaznacz pole wyboru **Zarządzanie magazynem wymiennym**.

Włóż kasety z taśmami do gniazd w bibliotece. Jeśli taśma nie ma kodu kreskowego lub jest on uszkodzony, etykietę taśmy w celu jej identyfikacji można określić później.

Na komputerze lokalnym lub na komputerach zdalnych należy zainstalować serwer Acronis Backup & Recovery 10 Management Server i konsolę Acronis Backup & Recovery 10 Management Console, a na komputerze, do którego jest podłączona biblioteka taśm, węzeł Acronis Backup & Recovery 10 Storage Node zarejestrowany na serwerze zarządzania.

Biblioteka taśm jako skarbiec zarządzany

Aby umożliwić wykonywanie operacji ochrony danych przy użyciu biblioteki plików, należy w niej utworzyć skarbiec zarządzany. Skarbiec można utworzyć w widoku konsoli **Skarbce centralne**. Więcej informacji można znaleźć w sekcji Tworzenie zarządzanego skarbca centralnego (s. 149).

Jednak najłatwiejszym sposobem jest utworzenie skarbca w widoku **Węzły magazynowania**. Następnie należy wybrać węzeł magazynowania, do którego jest podłączona biblioteka taśm i kliknąć **Utwórz skarbiec**. Program wyświetli stronę **Utwórz skarbiec centralny** z wstępnie wybranymi parametrami. Wystarczy podać nazwę skarbca w polu **Nazwa** i kliknąć **OK**.

Po utworzeniu skarbca jest on dostępny w widoku konsoli **Skarbce centralne**. Można teraz używać biblioteki taśm do tworzenia kopii zapasowych.

Program Acronis Backup & Recovery 10 umożliwia utworzenie tylko jednego skarbca na urządzeniu sieciowym.

Jeśli wszystkie kasety w bibliotece taśm mają kody kreskowe, a w puli **Wolny** systemu RSM znajduje się wystarczająca liczba taśm dla wybranego schematu tworzenia kopii zapasowych, biblioteka może działać w sposób całkowicie automatyczny.

Można rozpocząć używanie skarbca, nawet gdy wszystkie gniazda taśm są puste. Jeśli podczas tworzenia kopii zapasowej w gniazdach biblioteki nie ma dostępnych taśm, program wyświetli okno **Zadania wymagają działania użytkownika** z prośbą o załadowanie taśmy.

Jeśli nie można odczytać kodu kreskowego, program wyświetli okno **Zadania wymagają działania użytkownika** z prośbą o nadanie taśmie etykiety.

Czynności w skarbcu biblioteki taśm

Po wybraniu skarbca biblioteki taśm na panelu konsoli **Nawigacja**, na pasku narzędzi na stronie **Skarbce centralne** będą dostępne następujące dwie czynności stosowane tylko w odniesieniu do bibliotek taśm:

- **Zarządzaj taśmami** umożliwia wyświetlenie okna **Zarządzanie taśmami**, w którym można odświeżyć informacje na temat gniazd biblioteki, dokonać inwentaryzacji taśm umieszczonych w gniazdach i określić etykiety taśm. Po przypisaniu do taśmy nowej etykiety czynność ta umożliwia tymczasowe wysunięcie taśmy w celu zapisania etykiety na kasecie.
- **Skanuj ponownie taśmy** umożliwia wyświetlenie okna **Ponowne skanowanie taśm**, w którym można wybierać gniazda i uruchamiać procedurę Skanuj ponownie (s. 159) w celu odczytania specjalnych informacji dotyczących zawartości wybranych taśm.

Dla skarbca biblioteki taśm dostępne są także funkcje **Edytuj**, **Usuń**, **Sprawdź poprawność** i **Odśwież**.

Należy zaznaczyć, że te funkcje mają pewne specjalne cechy w przypadku biblioteki taśm. Operacja **Edytuj** umożliwia zastąpienie biblioteki taśm bez wykonywania operacji **Skanuj ponownie**. Operacja **Usuń** usuwa wszystkie informacje na temat wybranego skarbca biblioteki taśm z bazy danych węzła magazynowania, tj. operacja powoduje usunięcie zawartości wszystkich taśm za każdym razem, gdy dane są używane przez węzeł magazynowania na urządzeniu biblioteki taśm.

*Po wykonaniu operacji **Usuń** program usuwa zawartość skarbca z bazy danych węzła magazynowania bez uzyskiwania dostępu do taśm. Wykonanie planów i zadań wymagających użycia tego skarbca zakończy się niepowodzeniem.*

*Program usunie również archiwa kopii zapasowych należące do usuwanego skarbca centralnego w bibliotece taśm, ale te archiwa można odzyskać w dowolnym węźle magazynowania po wykonaniu operacji **Skanuj ponownie**.*

Czynności związane z archiwami na taśmach znajdujących się w bibliotece

Gdy bieżącym skarbcem jest biblioteka taśm, dostępne są następujące funkcje umożliwiające zarządzanie danymi w archiwum kopii zapasowych wybranym w widoku konsoli **Skarbce centralne**: **Sprawdź poprawność**, **Usuń**, **Usuń wszystkie archiwa**. Usuwanie z bazy danych węzła magazynowania nie wymaga uzyskania dostępu do taśm. Archiwum kopii zapasowych usunięte ze skarbca biblioteki można przywrócić przy użyciu operacji Skanuj ponownie (s. 159) wykonanej dla wszystkich taśm zawierających dane archiwum.

W przypadku taśmy, z której usunięto kopię zapasową, operacja **Skanuj ponownie** umożliwia odzyskanie kopii zapasowej, ponieważ powoduje odtworzenie informacji o zawartości kopii zapasowej w bazie danych węzła magazynowania.

Po usunięciu wszystkich kopii zapasowych z taśmy jest ona uważana za wolną. Dlatego po pierwszym zapisaniu danych na tej taśmie wszystkie usunięte kopie zapasowe są nieodwracalnie utracone.

Tworzenie kopii zapasowych w bibliotece taśm

Przy tworzeniu zasady/planu tworzenia kopii zapasowych, w których miejscem docelowym jest biblioteka taśm, tworzenie kopii zapasowych konfiguruje się w taki sam sposób, jak dla innych urządzeń pamięci. Jedyną różnicą są dodatkowe opcje Obsługa taśmy (s. 130), które można skonfigurować podczas tworzenia zasady/planu tworzenia kopii zapasowych. Opcje te umożliwiają określenie sposobu wykorzystania taśm w bibliotece przez zasadę/plan tworzenia kopii zapasowych,

jednak wstępnie ustawione wartości tych opcji zwiększają efektywność wykorzystania całej biblioteki oraz poszczególnych taśm.

Aby wyświetlić i zmienić opcje obsługi taśm, z górnego menu wybierz **Opcje > Domyślne opcje tworzenia kopii zapasowej i odzyskiwania > Domyślne opcje tworzenia kopii zapasowej > Obsługa taśmy**.

Aby zmienić ustawienia tworzonej zasady/planu tworzenia kopii zapasowej, kliknij **Zmień** w sekcji **Opcje tworzenia kopii zapasowej** na stronie **Utwórz zasady/plan tworzenia kopii zapasowych**. Program wyświetli okno **Opcje tworzenia kopii zapasowej** zawierające stronę **Obsługa taśmy**, na której są przedstawione wstępnie zdefiniowane wartości.

Jeśli taśma skończy się podczas tworzenia kopii zapasowej, program automatycznie zamontuje nową taśmę i operacja będzie kontynuowana na nowej taśmie.

Po uruchomieniu zadania tworzenia kopii zapasowej w konsoli są dostępne następujące informacje na temat taśm:

- liczba taśm używanych aktualnie przez operację tworzenia kopii zapasowej;
- w przypadku podziału kopii zapasowej etykiety taśm użytych przez zadanie do danej chwili;
- etykieta aktualnie zapisywanej taśmy.

Odzyskiwanie z biblioteki taśm

Odzyskiwanie danych z archiwów znajdujących się na urządzeniach taśmowych odbywa się w taki sam sposób, jak dla innych urządzeń pamięci.

Rozpocznij odzyskiwanie od utworzenia zadania odzyskiwania, następnie wybierz skarbiec na urządzeniu taśmowym i archiwum oraz kopię zapasową, z której chcesz odzyskać dane. Podczas tworzenia zadania program używa bazy danych węzła magazynowania zamiast bezpośredniego dostępu do taśm. Jednak wybranie danych do odzyskania (np. plików lub określonych woluminów) wymaga odczytania jednej lub kilku taśm, co może potrwać.

Program wyszukuje taśmy i ładuje je automatycznie we właściwej kolejności. Jeśli program nie znajdzie wymaganej taśmy, wyświetli okno **Zadania wymagają działania użytkownika**.

Należy pamiętać, że odzyskiwanie danych może wymagać uzyskania dostępu do kilku taśm. Odzyskiwanie danych z przyrostowej kopii zapasowej może na przykład wymagać ładowania, montowania, przewijania i odczytywania taśm zawierających kopie zapasowe danych:

- taśm zawierających przyrostowe kopie zapasowe wybrane do odzyskania danych;
- taśm zawierających ostatnią pełną kopię zapasową utworzoną wcześniej niż wybrana kopia przyrostowa;
- taśm zawierających ostatnią różnicową kopię zapasową utworzoną po ostatniej pełnej kopii zapasowej, ale przed utworzeniem wybranej kopii przyrostowej, jeśli to konieczne;
- taśm zawierających wszystkie przyrostowe kopie zapasowe utworzone po pełnych lub różnicowych kopiach zapasowych, ale przed utworzeniem wybranej kopii przyrostowej, jeśli to konieczne.

Po uruchomieniu zadania odzyskiwania w konsoli zarządzania są dostępne następujące informacje na temat taśm:

- etykiety wszystkich taśm wymaganych do operacji;
- etykieta aktualnie odczytywanej taśmy;
- etykiety już odczytanych taśm;

- etykiety taśm oczekujących na odczytanie oraz informacje na temat ich aktualnej dostępności (czy są załadowane czy nie).

Zarządzanie biblioteką taśm

W produkcie dostępne są następujące zadania/procedury umożliwiające zarządzanie biblioteką taśm:

- Inwentaryzacja (s. 159)
- Ponowne skanowanie (s. 159)
- Nadawanie etykiet (s. 160)

Operacje te może wykonać każdy użytkownik mający dostęp do skarbca zarządzanego w bibliotece taśm. Jednak kilku użytkowników nie może jednocześnie zarządzać biblioteką taśm, ponieważ wykonanie niektórych operacji trwa kilka minut, godzin lub nawet dni. Jeśli na przykład użytkownik uruchomi zadanie **Skanuj ponownie**, wówczas żądania wszystkich pozostałych użytkowników dotyczące wykonania tego samego zadania będą automatycznie anulowane, ponieważ jest ono już uruchomione w skarbcu.

Inwentaryzacja

Aby prawidłowo obsługiwać taśmy, w bazie danych węzła magazynowania muszą znajdować się informacje na ich temat. Dlatego po utworzeniu skarbca na ogół należy wykonać inwentaryzację.

Inwentaryzacja jest procedurą umożliwiającą węzłowi magazynowania rozpoznanie taśm załadowanych do gniazd biblioteki taśm. Jest to w miarę szybka procedura i zwykle wymaga odczytania kodów kreskowych kaset bez konieczności odczytywania danych na taśmie. Jeśli nie można odczytać kodu kreskowego, taśma jest montowana w celu odczytania wyłącznie identyfikatora GUID.

Procedurę **inwentaryzacji** można uruchomić ręcznie lub automatycznie, gdy jest wymagany dostęp do ostatnio dodanych taśm.

Aby uruchomić procedurę, wybierz skarbiec biblioteki taśm w panelu konsoli **Nawigacja**, kliknij **Zarządzaj taśmami**, a następnie kliknij **Rozpocznij inwentaryzację** w oknie **Zarządzanie taśmami**.

Po zakończeniu inwentaryzacji dostępna jest lista taśm załadowanych aktualnie do biblioteki.

Procedurę tę należy wykonać po każdym włożeniu nowych taśm do gniazd biblioteki.

Skanuj ponownie

Jak napisano powyżej, węzeł magazynowania przechowuje informacje na temat taśm i ich zawartości w dedykowanej bazie danych. Zadanie **Skanuj ponownie** odczytuje informacje na temat zawartości taśm wybranych przez użytkownika i aktualizuje bazę danych.

Wykonanie zadania może trwać długo, dlatego należy je zainicjować ręcznie. Przed uruchomieniem zadania należy wybrać wszystkie gniazda taśm do ponownego skanowania.

Zadanie **Skanuj ponownie** należy uruchomić:

- w przypadku nieznanych taśm w węźle magazynowania;
- po utraceniu lub uszkodzeniu bazy danych węzła magazynowania;
- w przypadku taśm, których zawartość jest nieaktualna (zmodyfikowanych na przykład przez inny węzeł magazynowania lub ręcznie).

Należy pamiętać, że taśma może zawierać kopie zapasowe usunięte przed jej ponownym skanowaniem. Po zakończeniu zadania program odzyska wszystkie takie kopie zapasowe w bazie danych węzła magazynowania. Będą one dostępne do odzyskiwania danych.

Po ponownym skanowaniu program zapisuje taśmę w bazie danych węzła magazynowania. Jeśli w gnieździe wybranym do tej procedury znajduje się taśma bez etykiety, program wstrzymuje zadanie **ponownego skanowania** w celu wykonania procedury nadawania etykiet (s. 160).

Nadawanie etykiet

Gdy program nie znajdzie taśmy wymaganej do odzyskania danych, wyświetli okno **Zadania wymagają działania użytkownika** i poprosi użytkownika o włożenie taśmy do gniazda biblioteki. Dlatego wszystkie kasety z taśmami muszą mieć kody kreskowe lub inne czytelne etykiety.

Jeśli taśma nie ma etykiety, należy ją nadać przed użyciem taśmy.

Aby zamiast kodu kreskowego nadać taśmie konkretną etykietę (na przykład etykietę „Praca” w przypadku taśmy przeznaczonej na kopie zapasowe plików z folderu C:\praca), również należy użyć procedury **nadawania etykiet**.

Aby uruchomić procedurę, wybierz skarbiec biblioteki taśm w panelu **Nawigacja** w konsoli i kliknij **Zarządzaj taśmami** na pasku narzędzi. W oknie **Zarządzanie taśmami** program wyświetli listę gniazd biblioteki zawierających taśmy. Jeśli w gnieździe znajduje się taśma z puli **Wolny** lub puli **Acronis**, w polu danych są dostępne informacje na temat etykiety taśmy. Etykiety są również wyświetlane dla taśm znajdujących się w puli **Importowany** i zawierają kopie zapasowe zapisane przez program Acronis. Taka sytuacja może zaistnieć podczas przenoszenia taśmy z innej biblioteki taśm.

Domyślnie nieużywana taśma z kodem kreskowym otrzymuje etykietę identyczną z kodem kreskowym. Jeśli taśma nie ma kodu kreskowego lub jest on uszkodzony, program automatycznie tworzy nazwę etykiety. Zaproponowaną etykietę można zaakceptować lub zastąpić własną w postaci zwykłego tekstu.

Nazwy taśm z puli **Wolny** lub **Importowany** można zmienić pod warunkiem, że konto użytkownika służące do uruchamiania usługi węzła magazynowania (**Użytkownik ASN**) ma uprawnienia zapisu do danych pul. Uprawnienia te nie są przypisywane do **Użytkownika ASN** w czasie instalacji, dlatego konieczne może być dodanie ich ręcznie.

W celu określenia własnej etykiety taśmy wybierz odpowiednie pole danych, wpisz nową etykietę, kliknij **Wysuń taśmę**, zapisz na kasecie z taśmą tę samą etykietę (aby ułatwić jej identyfikację) i włóż kasetę z powrotem do tego samego gniazda.

Gdy wszystkie wymagane etykiety taśm są już określone, naciśnij **Ustaw etykiety**, aby zapisać etykiety w bazie danych węzła magazynowania.

Obsługa taśmy

Opcje te są uwzględniane, gdy miejscem docelowym kopii zapasowej jest skarbiec zarządzany znajdujący się w bibliotece taśm.

Opcje **Obsługa taśmy** umożliwiają określenie sposobu dystrybucji kopii zapasowych na taśmach przez zadania tworzenia kopii zapasowych.

Niektóre kombinacje opcji dotyczących taśm mogą powodować zmniejszenie efektywności wykorzystania całej biblioteki lub poszczególnych taśm. Jeśli zmodyfikowanie tych opcji nie jest konieczne, należy pozostawić je bez zmian.

Archiwum może zajmować kilka taśm. Do przechowywania danych kopii zapasowych jest wtedy używany tzw. **zestaw taśm**.

Zestaw taśm jest to logiczna grupa składająca się z jednej lub kilku taśm zawierających kopie zapasowe określonych chronionych danych. Zestaw taśm może również zawierać kopie zapasowe innych danych.

Osobny zestaw taśm jest to zestaw zawierający tylko kopie zapasowe określonych chronionych danych. Nie można na nim zapisać innych kopii zapasowych.

(Dla tworzonej zasady/planu tworzenia kopii zapasowych) Użyj osobnego zestawu taśm

Ustawienie wstępne: **Wyłączone**.

Jeśli użytkownik nie zmieni tej opcji, kopie zapasowe należące do tworzonej zasady lub planu tworzenia kopii zapasowych można zapisywać na taśmach zwierających inne kopie zapasowe utworzone z danych z innych komputerów. Również kopie zapasowe utworzone przez inne zasady można zapisywać na taśmach zawierających kopie zapasowe utworzone przez daną zasadę. Nie ma problemu z takimi taśmami, ponieważ program wszystkimi taśmami zarządza automatycznie.

Po włączeniu tej opcji kopie zapasowe należące do tworzonej zasady lub planu tworzenia kopii zapasowych będą zapisywane na osobnym zestawie taśm, na którym nie będą zapisywane inne kopie zapasowe.

Gdy konsola jest podłączona do serwera zarządzania

Opcja **Użyj osobnego zestawu taśm** ma bardziej dokładną definicję. Dlatego w tworzonej zasadzie tworzenia kopii zapasowych można użyć osobnego zestawu taśm dla wszystkich komputerów lub dla każdego komputera osobno.

Opcja **Jeden zestaw taśm dla wszystkich komputerów** jest domyślnie wybrana. Ogólnie rzecz biorąc, opcja ta umożliwia bardziej efektywne wykorzystanie taśm niż opcja **Oddzielny zestaw taśm dla każdego komputera**. Jednak ta druga opcja może być przydatna, gdy na przykład istnieją specjalne wymagania dotyczące przechowywania taśm z kopiami zapasowymi danego komputera w innej lokalizacji.

Po włączeniu opcji **Użyj osobnego zestawu taśm** może wystąpić sytuacja, w której program chce zapisać kopię zapasową na taśmie, która aktualnie jest wyjęta z urządzenia biblioteki taśm. Należy określić sposób postępowania w takiej sytuacji.

- **Poproś o działanie użytkownika** — zadanie tworzenia kopii zapasowej przejdzie w stan **Wymagające działania** i będzie czekało na załadowanie do urządzenia biblioteki taśmy o odpowiedniej etykiecie.
- **Użyj wolnej taśmy** — program zapisze kopię zapasową na wolnej taśmie, dlatego operacja będzie wstrzymana tylko, gdy w bibliotece nie ma wolnych taśm.

Zawsze używaj wolnej taśmy

Jeśli użytkownik nie zmieni poniższych opcji, wszystkie kopie zapasowe będą zapisywane na taśmie określonej w opcji **Użyj osobnego zestawu taśm**. Po włączeniu niektórych z poniższych opcji program będzie dodawał nowe taśmy do zestawu taśm podczas każdej operacji tworzenia pełnej, przyrostowej lub różnicowej kopii zapasowej.

- **Do każdej pełnej kopii zapasowej**

Ustawienie wstępne: **Wyłączone**.

Po włączeniu tej opcji program zapisuje wszystkie pełne kopie zapasowe na wolnych taśmach. Taśma jest specjalnie ładowana do tej operacji. Gdy opcja **Użyj osobnego zestawu taśm** jest włączona,

program może dodać do taśmy tylko przyrostowe lub różnicowe kopie zapasowe tych samych danych.

- **Dla każdej różnicowej kopii zapasowej**

Ustawienie wstępne: **Wyłączone**.

Gdy ta opcja jest włączona, program zapisuje wszystkie różnicowe kopie zapasowe na wolnych taśmach. Ta opcja jest dostępna tylko, gdy dla wszystkich pełnych kopii zapasowych program używa wolnych taśm.

- **Do każdej przyrostowej kopii zapasowej**

Ustawienie wstępne: **Wyłączone**.

Gdy ta opcja jest włączona, program zapisuje wszystkie przyrostowe kopie zapasowe na wolnych taśmach. Ta opcja jest dostępna tylko, gdy dla wszystkich pełnych i różnicowych kopii zapasowych program używa wolnych taśm.

Rotacja taśm

Po usunięciu wszystkich kopii zapasowych z taśmy, na przykład skasowaniu informacji o ostatniej kopii zapasowej na taśmie z bazy danych węzła magazynowania, taśma jest uważana za pustą i można jej użyć w następnym cyklu tworzenia kopii zapasowych. Rotacja taśm umożliwia używanie minimalnej liczby kaset i ponowne wykorzystanie używanych taśm.

Program Acronis Backup & Recovery 10 umożliwia pełną automatyzację rotacji taśm podczas tworzenia kopii zapasowych w bibliotekach taśm.

Ta sekcja zawiera przydatne informacje dotyczące wyboru schematu tworzenia kopii zapasowych i opcji taśm związanych z rotacją.

W celu obliczenia liczby taśm wymaganych w schematach rotacji taśm można użyć metody opisanej w sekcji Planowanie taśm (s. 174).

Wybór schematu tworzenia kopii zapasowych

Podczas tworzenia zasady/planu tworzenia kopii zapasowych, w których miejscem docelowym jest biblioteka taśm, dostępne są następujące schematy tworzenia kopii zapasowych: **Utwórz kopię zapasową**, **Utwórz kopię zapasową później**, **Dziadek-ojciec-syn**, **Wieża Hanoi** lub **Niestandardowe**. Schemat **Prosty** jest niedostępny, ponieważ dla archiwów zapisanych na taśmach konsolidacja kopii zapasowych jest niemożliwa.

Program Acronis Backup & Recovery 10 umożliwia automatyzację rotacji taśm w schematach tworzenia kopii zapasowych **Dziadek-ojciec-syn**, **Wieża Hanoi** i **Niestandardowe**.

Dziadek-ojciec-syn (s. 38) (GFS) i Wieża Hanoi (s. 42) (ToH) to najpopularniejsze schematy tworzenia kopii zapasowych przy użyciu urządzeń biblioteki taśm. Schematy te są zoptymalizowane w celu zachowania najlepszej równowagi pomiędzy rozmiarem archiwum kopii zapasowej, liczbą punktów odzyskiwania dostępną w archiwum i liczbą taśm wymaganych do archiwizowania.

Jeśli archiwum kopii zapasowych jest używane w celu odzyskiwania danych z codziennych kopii zapasowych z co najmniej kilku ostatnich dni, cotygodniowych kopii z co najmniej kilku ostatnich tygodni, lub comiesięcznych kopii z dowolnego okresu w przeszłości, preferowanym schematem jest **Dziadek-ojciec-syn**.

Jeśli głównym celem jest zapewnienie ochrony danych przez jak najdłuższy czas przy użyciu minimalnej liczby taśm załadowanych do niewielkiej biblioteki (np. automatycznego urządzenia ładującego), najlepszym rozwiązaniem jest użycie schematu **Wieża Hanoi**.

Schemat tworzenia kopii zapasowych **Niestandardowe** umożliwia określenie harmonogramu tworzenia kopii zapasowych i reguł przechowywania w celu zdefiniowania żądanej rotacji taśm. Tego schematu należy użyć, gdy użycie schematów **Dziadek-ojciec-syn** i **Wieża Hanoi** jest niewystarczające. Jeśli na przykład całkowity rozmiar chronionych danych jest znacząco mniejszy od rozmiaru taśmy, najlepszym rozwiązaniem jest użycie schematu **Niestandardowe** z regularnym tworzeniem pełnych kopii codziennie/co tydzień/co miesiąc, prostymi regułami przechowywania i domyślnymi opcjami taśm.

Kryteria wyboru

Przed każdym utworzeniem schematu rotacji taśm dla zasady/planu tworzenia kopii zapasowych należy wziąć pod uwagę następujące czynniki:

- całkowity rozmiar chronionych danych;
- przybliżony rozmiar danych zmienianych codziennie;
- przybliżony rozmiar danych zmienianych co tydzień;
- wymagania dotyczące schematu tworzenia kopii zapasowych (częstotliwość, wydajność i czas trwania operacji tworzenia kopii zapasowych);
- wymagania dotyczące przechowywania kopii zapasowych (minimalny/maksymalny okres przechowywania kopii, wymagania związane z przechowywaniem kaset w innej lokalizacji);
- możliwości biblioteki taśm (liczba napędów, urządzeń ładujących, gniazd i dostępnych taśm oraz pojemność taśm);
- wymagania związane z odzyskiwaniem danych (maksymalny czas trwania).

Należy przeanalizować wszystkie istotne czynniki w danym przypadku i określić główne kryteria wyboru. Następnie można wybrać schemat tworzenia kopii zapasowych i opcje dotyczące taśm.

Należy pamiętać, że każdy schemat tworzenia kopii zapasowych w połączeniu z różnymi opcjami dotyczącymi taśm może dać zupełnie odmienne rezultaty związane z efektywnym wykorzystaniem zarówno taśm, jak i urządzeń.

Przykład do analizy

Załóżmy, że chcemy zautomatyzować rotację taśm w następującej sytuacji:

- Całkowity rozmiar chronionych danych wynosi około 320 GB.
- Przybliżony rozmiar danych zmienianych codziennie wynosi około 16 GB.
- Przybliżony rozmiar danych zmienianych co tydzień nie przekracza 40 GB.
- Pojemność taśmy wynosi 400 GB.

Przeanalizujmy efekty połączenia schematów Dziadek-ojciec-syn i Wieża Hanoi z różnymi opcjami taśm dla tego przypadku.

Wszystkie przeanalizowane poniżej przykłady są uproszczone, ale obrazują ogólną zasadę rozkładu kopii zapasowych na taśmach.

Legenda do rysunków związanych z przykładami

Codzienna/przyrostowa kopia zapasowa (16 GB) jest przedstawiona jako zielony prostokąt:  .

Cotygodniowa/ różnicowa kopia zapasowa (40 GB) jest przedstawiona jako niebieski prostokąt:  .

Pełna comiesięczna kopia zapasowa (320 GB) jest przedstawiona jako pomarańczowy prostokąt:

 .

Cała taśma (400 GB) jest przedstawiona jako szary prostokąt:

 .

Używanie schematu rotacji taśm Dziadek-ojciec-syn (GFS)

Sposób rotacji taśm w schemacie Dziadek-ojciec-syn jest określony głównie przez opcje taśm określone w tworzonej zasadzie/planie tworzenia kopii zapasowych.

Przyjmijmy następujące ustawienia dla schematu Dziadek-ojciec-syn:

- **Rozpocznij tworzenie kopii zapasowej o:** **23:00:00**
- **Utwórz kopię zapasową dnia:** **Dni robocze**
- **Tygodniowa/miesięczna:** **Piątek**
- **Zachowuj kopie zapasowe: Codziennie:** **2 tygodnie, Co tydzień: 2 miesiące, Co miesiąc: 1 rok**.

Głównym celem jest osiągnięcie pełnej automatyzacji rotacji taśm przy tych ustawieniach.

Należy pamiętać, że w tym schemacie Dziadek-ojciec-syn co miesiąc jest tworzona pełna kopia zapasowa, co tydzień kopia różnicowa, a codziennie kopia przyrostowa. Pierwsza kopia zapasowa jest zawsze pełna. Zatem jeśli zasada/plan tworzenia kopii zapasowych zostaną uruchomione w środę, a pełne kopie zapasowe program ma tworzyć co czwarty piątek, kopia utworzona w środę będzie pełna, a nie przyrostowa.

Przeanalizowane przykłady zakładające użycie schematu Dziadek-ojciec-syn w połączeniu z różnymi opcjami taśm są opisane w następujących sekcjach:

- Dziadek-ojciec-syn — Przykład 1 (s. 164). Opcja **Użyj osobnego zestawu taśm** jest wybrana. Żadna z opcji **Zawsze używaj wolnej taśmy** nie jest wybrana. Schemat wymaga rotacji 25 taśm.
- Dziadek-ojciec-syn — Przykład 2 (s. 168). Opcja **Użyj osobnego zestawu taśm** jest wybrana. Opcja **Zawsze używaj wolnej taśmy: Do każdej pełnej kopii zapasowej** jest wybrana. Pozostałe opcje **Zawsze używaj wolnej taśmy** nie są wybrane. Schemat wymaga rotacji 16 taśm.
- Dziadek-ojciec-syn — Przykład 3 (s. 169). Opcja **Użyj osobnego zestawu taśm** jest wybrana. Wszystkie opcje **Zawsze używaj wolnej taśmy** są wybrane. Schemat wymaga rotacji 28 taśm.

Przykłady te ilustrują wpływ opcji dotyczących taśm na liczbę taśm wymaganych do automatycznej rotacji. Jeśli w bibliotece nie ma wystarczającej liczby taśm do automatycznej rotacji, program będzie czasem wyświetlał okno **Zadania wymagają działania użytkownika** z prośbą o załadowanie do biblioteki wolnej taśmy.

Dziadek-ojciec-syn — Przykład 1

Przypuśćmy, że w planie tworzenia kopii zapasowych ustawiono następujące opcje dotyczące taśm:

- Opcja **Użyj osobnego zestawu taśm** jest wybrana.
- Opcja **Zawsze używaj wolnej taśmy: Do każdej pełnej kopii zapasowej** nie jest wybrana.
- Opcja **Zawsze używaj wolnej taśmy: Do każdej przyrostowej kopii zapasowej** nie jest wybrana.

- Opcja **Zawsze używaj wolnej taśmy: Dla każdej różnicowej kopii zapasowej** nie jest wybrana.

Przyjmijmy, że pierwsza operacja utworzenia kopii zapasowej ma się rozpocząć w piątek, 1 stycznia. W tym dniu o godzinie 23.00 program utworzy pierwszą pełną kopię zapasową (320 GB na taśmie o pojemności 400 GB). Ponieważ wybrana jest opcja **Użyj osobnego zestawu taśm**, program wysunie aktualnie zamontowaną taśmę (jeśli nie jest to wolna taśma). Następnie program załaduje specjalną taśmę do utworzenia kopii zapasowej danych. Ta taśma ma numer 01 na poniższym rysunku. Zgodnie z legendą opisaną w sekcji Przykład do analizy (s. 163), pełna kopia zapasowa danych jest przedstawiona na rysunku jako pomarańczowy prostokąt.

Wybrane ustawienia schematu Dziadek-ojciec-syn wymuszają tworzenie kopii zapasowych tylko w **Dni robocze**, dlatego kolejną kopię zapasową program utworzy o tej samej godzinie (**23.00**) w poniedziałek, 4 stycznia. Jest to kopia przyrostowa (16 GB) zapisana na tej samej taśmie 01, ponieważ opcja **Zawsze używaj wolnej taśmy: Do każdej przyrostowej kopii zapasowej** nie jest wybrana. Ta kopia zapasowa jest przedstawiona na rysunku jako zielony prostokąt.

Program zapisze na taśmie 01 kolejne trzy przyrostowe kopie zapasowe w dniach: 5, 6 i 7 stycznia. W rezultacie na taśmie pozostanie tylko 16 GB wolnego miejsca.

8 stycznia program zapisze dane różnicowej kopii zapasowej (40 GB) na tej samej taśmie 01, ponieważ opcja **Zawsze używaj wolnej taśmy: Dla każdej różnicowej kopii zapasowej** nie jest wybrana. Jednak taśma skończy się po zapisaniu pierwszych 16 GB kopii zapasowej. Program odmontuje taśmę i wysunie ją z napędu, a urządzenie ładujące umieści ją w gnieździe. Następnie do tego samego napędu zostanie załadowana wolna taśma, program zamontuje ją i tworzenie kopii zapasowej (ostatnie 24 GB) będzie kontynuowane przy użyciu nowej taśmy.

Na kolejnym rysunku pokazano wygląd kopii zapasowej danych w tym momencie. Różnicowa kopia zapasowa jest przedstawiona na rysunku jako niebieski prostokąt. Numer 1 na zielonym prostokącie oznacza przyrostową kopię zapasową utworzoną w poniedziałek, pierwszego tygodnia w danym roku.

Na taśmie 02 program zapisze następujące kopie zapasowe:

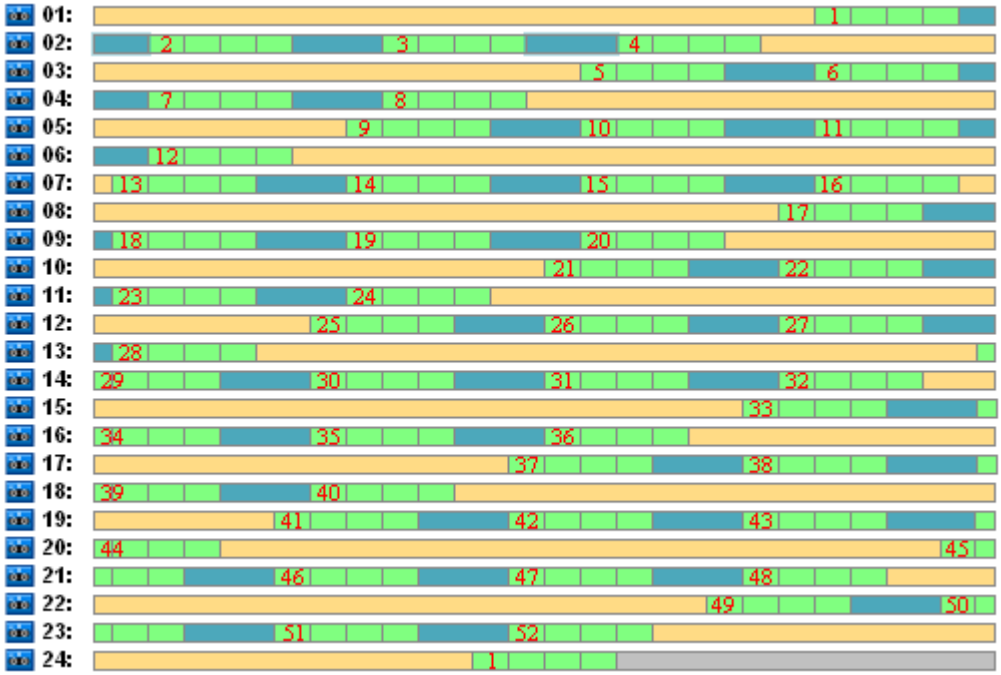
- cztery kopie przyrostowe i jedną kopię różnicową w drugim tygodniu,
- cztery kopie przyrostowe i jedną kopię różnicową w trzecim tygodniu,
- cztery kopie przyrostowe w czwartym tygodniu.

Kolejną pełną kopię zapasową (320 GB) program powinien zapisać w piątek w czwartym tygodniu. Jednak na taśmie 02 pozostało tylko 104 GB wolnego miejsca. Zatem po osiągnięciu końca taśmy program kontynuuje nagrywanie od początku taśmy 03.

Należy pamiętać, że po utworzeniu każdej kopii zapasowej w schemacie Dziadek-ojciec-syn program uruchamia zadanie **Czyszczenie**. Zadanie to usuwa wszystkie przestarzałe kopie zapasowe. Na kolejnym rysunku w miejscu usuniętych kopii zapasowych przedstawiono ciemnoszare prostokąty.

Usunięte kopie zapasowe znajdują się nadal fizycznie na taśmach, ale program usuwa informacje na temat tych kopii z bazy danych węzła magazynowania.

Na poniższym rysunku usunięte kopie zapasowe są pokazane jako rzeczywiste, ale rysunek przedstawia wykorzystanie taśm przez cały rok w schemacie Dziadek-ojciec-syn, przy określonych ustawieniach opcji związanych z taśmami. Liczby w zielonych prostokątach oznaczają przyrostowe kopie zapasowe utworzone w poniedziałki, w kolejnych tygodniach roku.



Wykorzystanie taśm w ciągu pierwszego roku

Kolejny rysunek przedstawia rzeczywiste wykorzystanie taśm z wolnym miejscem po usunięciu kopii zapasowych w pierwszy piątek kolejnego roku. Na taśmie 24 program zapisał wówczas różnicową kopię zapasową (niebieski prostokąt).

Program usunie pełną kopię zapasową na taśmie 01 po utworzeniu kolejnej pełnej kopii zapasowej na taśmach 23 i 24 w piątek, w 52 tygodniu roku. Ponieważ na taśmie 01 nie ma już żadnych kopii, jest ona uważana za wolną i można jej ponownie użyć.

Z dalszej analizy przykładu wynika, że maksymalna liczba taśm wymaganych do zapisania kopii zapasowych danych wynosi 25. To maksimum zostaje osiągnięte w 16 tygodniu następnego roku.

Przedstawione powyżej rysunki pokazują, że odzyskiwanie danych wymaga użycia jednej lub dwóch taśm dla pełnej kopii zapasowej, dwóch lub trzech taśm dla różnicowej kopii zapasowej i jednej, dwóch lub trzech taśm dla przyrostowej kopii zapasowej.

Jeśli na przykład zaistnieje konieczność odzyskania danych z kopii zapasowej utworzonej w poniedziałek w 52 tygodniu roku, zadanie będzie wymagało użycia trzech taśm:

- taśmy 23 zawierającej przyrostową kopię zapasową (o numerze „52”) oraz różnicową kopię zapasową utworzoną w piątek w 51 tygodniu roku;
- taśm 21 i 22 zawierających pełną kopię zapasową utworzoną w piątek w 48 tygodniu roku.

Na podstawie tego przykładu można wskazać następujące wady użycia schematu w połączeniu z wybranymi opcjami dotyczącymi taśm:

- odzyskiwanie danych jest zwykle czasochłonne i wymaga ładowania, montowania, przewijania i odczytywania jednej (dla 3% kopii zapasowych na rysunku „Wykorzystanie taśm w ciągu pierwszego roku”), dwóch (65%) lub trzech (32%) taśm;
- do przechowywania 13 pełnych miesięcznych kopii zapasowych są używane 22 taśmy, podczas gdy rozmiar miesięcznej kopii zapasowej jest mniejszy od pojemności taśmy, zatem przechowywanie danych kosztuje więcej;
- do całorocznej rotacji kopii zapasowych danych wymagane jest użycie 25 taśm.

Dziadek-ojciec-syn — Przykład 2

Przypuśćmy, że w planie tworzenia kopii zapasowych ustawiono następujące opcje dotyczące taśm:

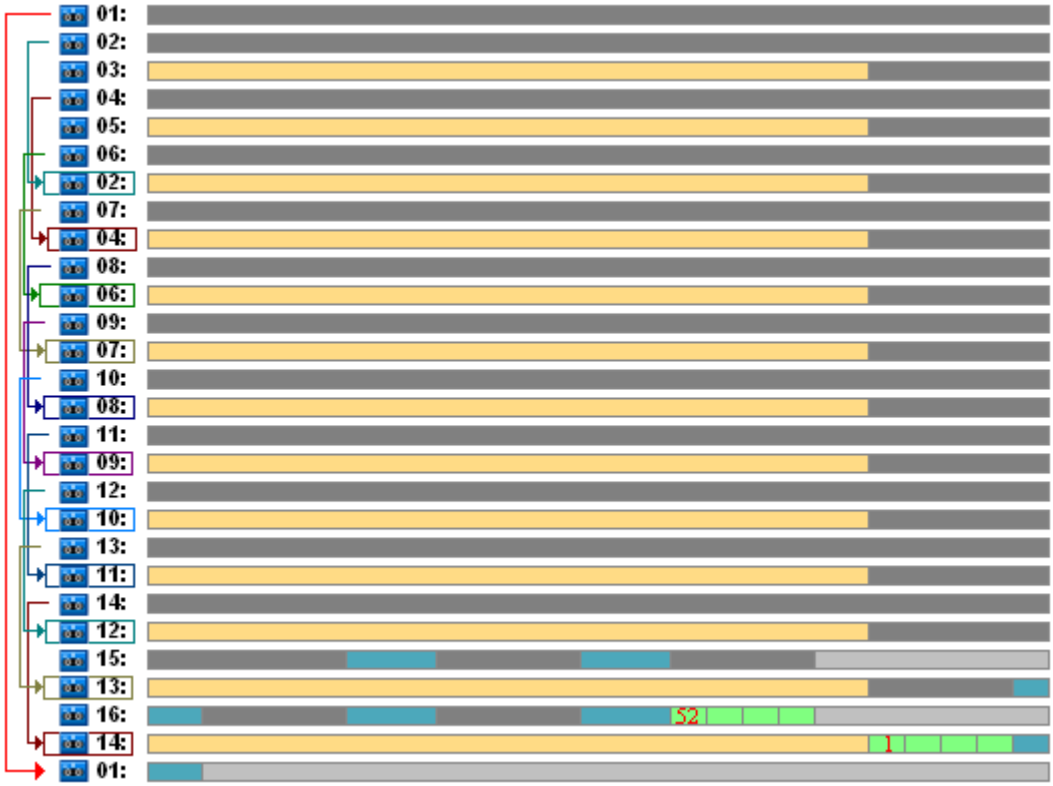
- Opcja **Użyj osobnego zestawu taśm** jest wybrana.
- Opcja **Zawsze używaj wolnej taśmy: Do każdej pełnej kopii zapasowej** jest wybrana.
- Opcja **Zawsze używaj wolnej taśmy: Do każdej przyrostowej kopii zapasowej** nie jest wybrana.
- Opcja **Zawsze używaj wolnej taśmy: Dla każdej różnicowej kopii zapasowej** nie jest wybrana.

Ten przykład różni się od poprzedniego tylko jednym szczegółem: opcja **Zawsze używaj wolnej taśmy: Do każdej pełnej kopii zapasowej** jest teraz wybrana.

Na poniższym rysunku usunięte kopie zapasowe są pokazane jako rzeczywiste, ale rysunek przedstawia wykorzystanie taśm przez cały rok w schemacie Dziadek-ojciec-syn, przy określonych ustawieniach opcji związanych z taśmami. Liczby w zielonych prostokątach oznaczają przyrostowe kopie zapasowe utworzone w poniedziałki, w kolejnych tygodniach roku.

Jeśli istnieje konieczność przechowywania wszystkich kopii zapasowych przez cały rok, archiwum będzie wymagało użycia 28 taśm.

Ponieważ schemat Dziadek-ojciec-syn wymusza automatyczne usunięcie przestarzałych kopii zapasowych, w pierwszy piątek drugiego roku na taśmach będą dostępne tylko kopie zapasowe przedstawione na poniższym rysunku.



Z rysunku wynika, że schemat rotacji taśm w **Przykładzie 2** jest bardziej odpowiedni dla tej sytuacji, niż schemat przedstawiony w **Przykładzie 1**. Schemat rotacji taśm w **Przykładzie 2** ma następujące zalety w analizowanym przypadku:

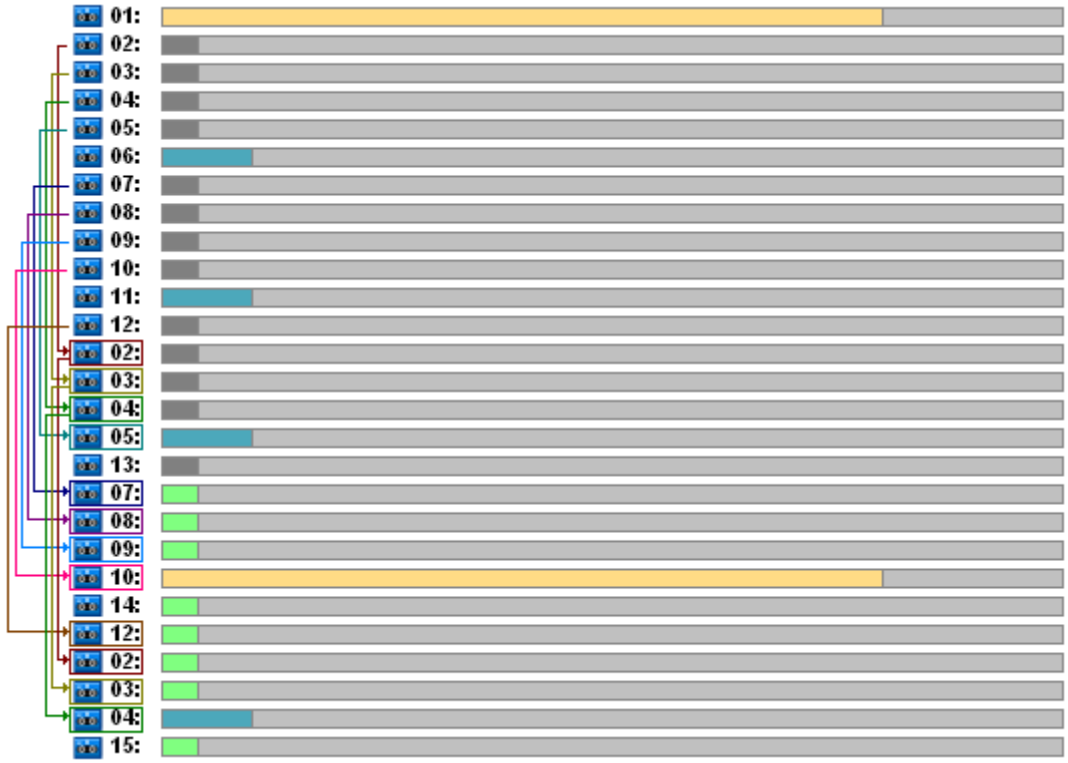
- używa 16 taśm zamiast 25;
- odzyskiwanie danych wymaga użycia jednej (25%) lub dwóch taśm (75%);
- odzyskiwanie danych z pełnej kopii zapasowej wymaga użycia tylko jednej taśmy, co przyspiesza odzyskiwanie danych z kopii przyrostowych i różnicowych.

Dziadek-ojciec-syn — Przykład 3

Przypuśćmy, że w planie tworzenia kopii zapasowych ustawiono następujące opcje dotyczące taśm:

- Opcja **Użyj osobnego zestawu taśm** jest wybrana.
- Opcja **Zawsze używaj wolnej taśmy: Do każdej pełnej kopii zapasowej** jest wybrana.
- Opcja **Zawsze używaj wolnej taśmy: Do każdej przyrostowej kopii zapasowej** jest wybrana.
- Opcja **Zawsze używaj wolnej taśmy: Dla każdej różnicowej kopii zapasowej** jest wybrana.

Te opcje określają klasyczny sposób rotacji taśm dla schematu Dziadek-ojciec-syn. Rysunek przedstawia początek schematu rotacji w analizowanej sytuacji, używającego 8 taśm dla codziennych kopii zapasowych, 6 taśm dla cotygodniowych kopii zapasowych i 13 taśm dla miesięcznych kopii zapasowych (ponieważ w roku występuje 13 cykli po 4 tygodnie). Wymagana jest jeszcze jedna taśma dla kolejnej kopii zapasowej. W sumie w tym schemacie rotacji, dla wybranych opcji wymagane jest użycie 28 taśm.



W celu odzyskania danych wymagane jest użycie tylko jednej taśmy dla pełnej kopii zapasowej, dwóch taśm dla różnicowej kopii zapasowej i dwóch lub trzech taśm dla przyrostowej kopii zapasowej.

Ten schemat ma następujące zalety:

- dostęp do dowolnej pełnej kopii zapasowej wymaga użycia tylko jednej taśmy;
- usunięcie kopii zapasowej powoduje zwolnienie taśmy, którą można ponownie użyć.

Główną wadą jest duża liczba taśm wykorzystanych w zaledwie 5-10%.

Jeśli codzienne kopie zapasowe należy przechowywać przez tydzień (4 kopie zapasowe), a cotygodniowe kopie zapasowe przez miesiąc (4 kopie zapasowe), łączna liczba taśm będzie wynosiła 4+4+13+1 = 22.

Używanie schematu rotacji taśm Wieża Hanoi (ToH)

Schemat Wieża Hanoi wymaga do rotacji mniejszej liczby taśm w porównaniu ze schematem Dziadek-ojciec-syn. Zatem schemat Wieża Hanoi jest optymalnym wyborem w małych bibliotekach taśm, a zwłaszcza w przypadku zmieniaczy.

Po wybraniu schematu tworzenia kopii zapasowych Wieża Hanoi można określić harmonogram schematu oraz liczbę poziomów.

Ze sprawdzonych sposobów postępowania wynika, że jeśli schemat Wieża Hanoi jest stosowany do tworzenia tygodniowych kopii zapasowych, należy użyć pięciu poziomów, a jeśli jest on stosowany do tworzenia kopii dziennych, należy użyć ośmiu poziomów. W pierwszym przypadku rotacja obejmuje 16 tygodniowych sesji i zapewnia okres wycofywania (minimalną liczbę dni, o którą można się cofnąć w zakresie archiwum) wynoszący 8 tygodni. Rotacja taśm w drugim przypadku obejmuje 128 sesji dziennych i zapewnia okres wycofywania wynoszący 64 dni. Okres wycofywania jest zawsze równy połowie liczby sesji.

Każdy dodatkowy poziom powoduje podwojenie nie tylko liczby sesji, ale również wieku najstarszej kopii zapasowej.

Powróćmy do sytuacji opisanej w sekcji Przykład do analizy (s. 163) i załóżmy następujące ustawienia schematu Wieża Hanoi:

- **Harmonogram:** **Rozpocznij zadanie co 1 dzień o 23:00. Powtórz raz.**
- **Liczba poziomów:** **5**

Schemat Wieża Hanoi z pięcioma poziomami zapewnia okres wycofywania wynoszący 8 dni. Do kopii zapasowych na poziomach od 1 do 5 przypiszmy litery odpowiednio A, B, C, D i E. Wzór rotacji dla sekwencji tworzenia kopii zapasowych w archiwum jest następujący: E-A-B-A-C-A-B-A-D-A-B-A-C-A-B-A. W pięciopoziomowym schemacie Wieża Hanoi wszystkie kopie zapasowe na 1 poziomie (A) są przyrostowe, na 5 poziomie (E) — pełne, a pozostałe kopie na poziomach 2, 3 i 4 (B, C i D) są różnicowe.

Rotacja taśm w schemacie Wieża Hanoi w dużej mierze zależy od opcji taśm, których domyślne ustawienia nie zawsze zapewniają optymalne wykorzystanie taśm i całej biblioteki.

Celem jest wybranie ustawień opcji taśm, które wymagają użycia minimalnej liczy taśm do rotacji.

Przykładowe analizy przedstawiające użycie schematu Wieża Hanoi w powiązaniu z różnymi opcjami taśm są opisane w następujących sekcjach:

- Wieża Hanoi — przykład 1. (s. 171) Opcja **Użyj osobnego zestawu taśm** jest wybrana. Żadna z opcji **Zawsze używaj wolnej taśmy** nie jest wybrana. Schemat wymaga rotacji 5 taśm.
- Wieża Hanoi — przykład 2 (s. 172). Opcja **Użyj osobnego zestawu taśm** jest wybrana. Opcja **Zawsze używaj wolnej taśmy: Do każdej pełnej kopii zapasowej** jest wybrana. Pozostałe opcje **Zawsze używaj wolnej taśmy** nie są wybrane. Schemat wymaga rotacji 4 taśm.
- Wieża Hanoi — przykład 3. (s. 173) Opcja **Użyj osobnego zestawu taśm** jest wybrana. Wszystkie opcje **Zawsze używaj wolnej taśmy** są wybrane. Schemat wymaga rotacji 7 taśm.

W przykładzie 2 schematu Wieża Hanoi należy użyć 4 taśm, co stanowi minimum w analizowanym przypadku. Dlatego ustawienia opcji taśm wybrane w tym przykładzie są najlepsze na tle ustawień w innych przykładach.

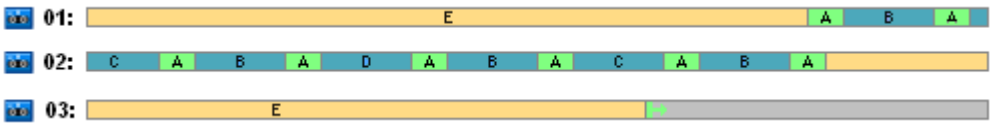
Wieża Hanoi — Przykład 1

Przypuśćmy, że w planie tworzenia kopii zapasowych ustawiono następujące opcje dotyczące taśm:

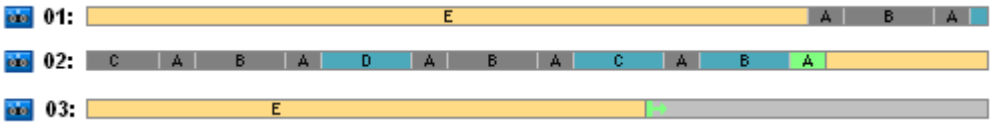
- Opcja **Użyj osobnego zestawu taśm** jest wybrana.
- Opcja **Zawsze używaj wolnej taśmy: Do każdej pełnej kopii zapasowej** nie jest wybrana.
- Opcja **Zawsze używaj wolnej taśmy: Do każdej przyrostowej kopii zapasowej** nie jest wybrana.
- Opcja **Zawsze używaj wolnej taśmy: Dla każdej różnicowej kopii zapasowej** nie jest wybrana.

Poniższy rysunek przedstawia wykorzystanie taśm w schemacie Wieża Hanoi w połączeniu z podanymi powyżej opcjami. Powtarzająca się część schematu obejmuje szesnaście sesji tworzenia

kopii zapasowych. Na rysunku jest przedstawiony stan archiwum kopii zapasowej po zakończeniu 17 sesji.

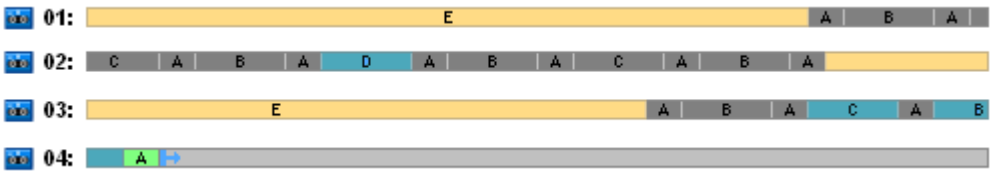


Ponieważ schemat tworzenia kopii zapasowych Wieża Hanoi wymusza obecność tylko jednej kopii zapasowej na każdym poziomie, wszystkie przestarzałe kopie zapasowe są automatycznie usuwane. Na kolejnym rysunku usunięte kopie zapasowe są przedstawione jako ciemnoszare prostokąty. W rzeczywistości usunięte kopie zapasowe nadal znajdują się na taśmach, ale informacje o nich są usunięte z bazy danych węzła magazynowania.



Rysunek przedstawia pełną kopię zapasową zapisaną na taśmie 01, której nie można usunąć, ponieważ stanowi podstawę dla kopii różnicowych (D, C, B) i kopii przyrostowej (A) zapisanych na taśmie 02. Usunięcie pełnej kopii zapasowej jest wstrzymane do czasu usunięcia wymienionych czterech kopii zapasowych.

Kolejny rysunek przedstawia zawartość taśm przed utworzeniem nowej kopii zapasowej na poziomie D:



Obecnie archiwum danych zajmuje cztery taśmy, a łączny rozmiar zapisanych do tej pory kopii zapasowych jest maksymalny dla tego przykładu. Jednak w przyszłości na końcu taśmy program zapisze pełną kopię zapasową i archiwum będzie zajmowało pięć taśm.

Po utworzeniu kolejnej kopii zapasowej na poziomie D program zwolni taśmę 01 i będzie mógł jej ponownie użyć.

Należy zauważyć, że w analizowanej sytuacji użycie schematu Wieża Hanoi wraz z określonymi opcjami przyniosło następujący efekt:

- z ostatniego rysunku wynika, że odzyskanie danych wymaga załadowania i zamontowania do trzech taśm (jedna taśma — 16%, dwie taśmy — 72%, trzy taśmy — 12%), a także przewinięcia i odczytania jednej (6%), dwóch (50%) lub trzech (44%) kopii zapasowych;
- w tym przypadku schemat o pięciu poziomach wymaga użycia pięciu taśm.

Wieża Hanoi — Przykład 2

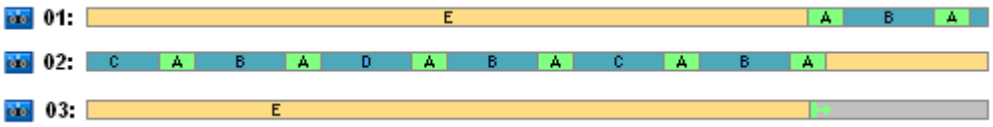
Przypuśćmy, że w planie tworzenia kopii zapasowych ustawiono następujące opcje dotyczące taśm:

- Opcja **Użyj osobnego zestawu taśm** jest wybrana.
- Opcja **Zawsze używaj wolnej taśmy: Do każdej pełnej kopii zapasowej** jest wybrana.
- Opcja **Zawsze używaj wolnej taśmy: Do każdej przyrostowej kopii zapasowej** nie jest wybrana.

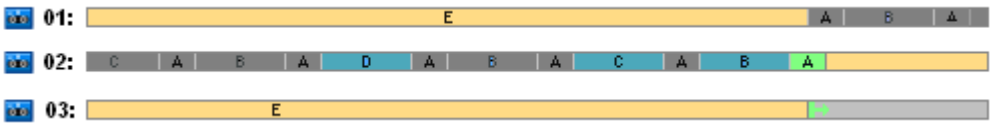
- Opcja **Zawsze używaj wolnej taśmy: Dla każdej różnicowej kopii zapasowej** nie jest wybrana.

Jedyną różnicą pomiędzy **Przykładem 2** a **Przykładem 1** jest wybranie opcji **Zawsze używaj wolnej taśmy: Do każdej pełnej kopii zapasowej**.

Pierwszy rysunek przedstawia wykorzystanie taśm w schemacie Wieża Hanoi w połączeniu z podanymi powyżej opcjami. Powtarzająca się część schematu obejmuje szesnaście sesji tworzenia kopii zapasowych. Na rysunku jest przedstawiony stan archiwum kopii zapasowej po zakończeniu 17 sesji.



Na poniższym rysunku usunięte kopie zapasowe są przedstawione jako ciemnoszare prostokąty.



Z rysunku wynika, że w danej chwili istnieją dwie pełne kopie zapasowe na poziomie E, ponieważ pierwsza pełna kopia zapasowa stanowi podstawę dla różnicowych kopii zapasowych D, C i B, które stanowią podstawę dla kopii przyrostowej A. Zatem usunięcie pełnej kopii zapasowej jest wstrzymane do momentu usunięcia kopii zapasowych D, C, B i A.

Kolejny rysunek przedstawia zawartość taśm przed utworzeniem nowej kopii zapasowej na poziomie D:

Obecnie archiwum kopii zapasowych zajmuje cztery taśmy. Jest to maksymalna liczba taśm wymaganych w tym przykładzie.

Po utworzeniu kolejnej kopii zapasowej na poziomie D program zwolni taśmy 01 i 02 i będzie mógł ich ponownie użyć.

Należy zauważyć, że w analizowanej sytuacji użycie schematu Wieża Hanoi wraz z określonymi opcjami przyniosło następujący efekt:

- odzyskanie danych wymaga uzyskania dostępu do kopii zapasowych zapisanych na jednej (25%) lub dwóch (75%) taśmach,
- pięciopoziomowy schemat może wymagać użycia do czterech taśm.

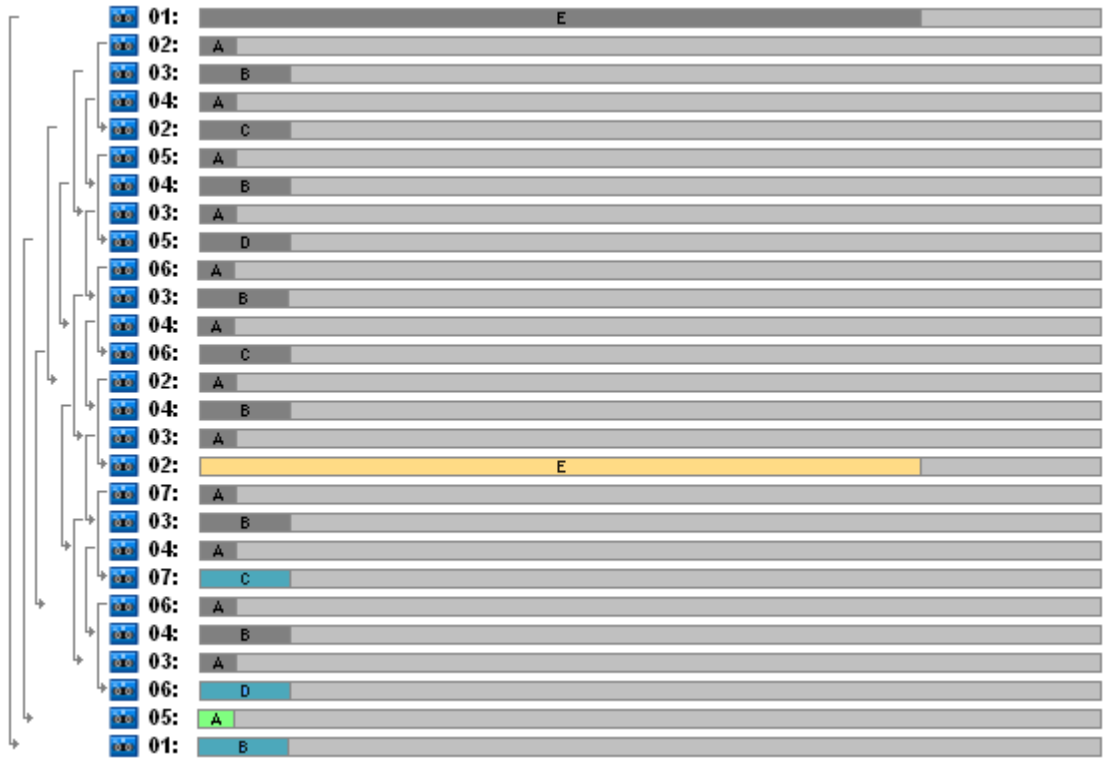
Zatem w przedstawionym przykładzie wybranie opcji **Zawsze używaj wolnej taśmy: Do każdej pełnej kopii zapasowej** znacząco zwiększa efektywność wykorzystania taśm w bibliotece.

Wieża Hanoi — Przykład 3

Przypuśćmy, że w planie tworzenia kopii zapasowych ustawiono następujące opcje dotyczące taśm:

- Opcja **Użyj osobnego zestawu taśm** jest wybrana.
- Opcja **Zawsze używaj wolnej taśmy: Do każdej pełnej kopii zapasowej** jest wybrana.
- Opcja **Zawsze używaj wolnej taśmy: Do każdej przyrostowej kopii zapasowej** jest wybrana.
- Opcja **Zawsze używaj wolnej taśmy: Dla każdej różnicowej kopii zapasowej** jest wybrana.

Rysunek przedstawia rotację taśm w schemacie Wieża Hanoi z wybranymi powyższymi opcjami.



Maksymalna liczba taśm używanych do rotacji wynosi siedem, czyli więcej niż w klasycznym pięciopoziomowym schemacie Wieża Hanoi.

Dwie dodatkowe taśmy są używane w celu :

1. przechowywania starej pełnej kopii zapasowej (wstrzymane usunięcie), stanowiącej podstawę dla kopii zapasowych innych poziomów;
2. przechowywania starej kopii zapasowej na danym poziomie do czasu utworzenia nowej kopii zapasowej na tym poziomie.

W tym przykładzie efektywność wykorzystania taśm jest mniejsza. Odzyskanie danych wymaga uzyskania dostępu do kopii zapasowych zapisanych na jednej taśmie (pełne kopie zapasowe, 6%), dwóch taśmach (różnicowe kopie zapasowe, 44%) lub trzech taśmach (przyrostowe kopie zapasowe, 50%). Zatem operacja zajmuje średnio więcej czasu niż w poprzednich przykładach.

Planowanie taśm

Po określeniu schematu tworzenia kopii zapasowych i opcji używania taśm należy określić minimalną liczbę taśm niezbędnych do uzyskania pełnej automatyzacji rotacji taśm.

W celu uproszczenia planowania taśm pomińmy możliwość, że na taśmach mogą znajdować się kopie zapasowe innych danych. Przyjmijmy, że opcja **Użyj osobnego zestawu taśm** jest włączona.

Aby obliczyć liczbę taśm, należy rozważyć następujące czynniki:

- rozmiar pełnej kopii zapasowej;
- średni rozmiar przyrostowych kopii zapasowych;
- średni rozmiar różnicowych kopii zapasowych;
- poziom kompresji określony dla tworzenia kopii zapasowych danych;
- schemat rotacji taśm (częstotliwość tworzenia kopii zapasowych, reguły przechowywania);
- opcje dołączania taśm;
- wymagania dotyczące obsługi archiwów taśm zainstalowanych w innej lokalizacji.

Nie istnieje ogólny wzór umożliwiający obliczenie liczby taśm wymaganych we wszystkich możliwych kombinacjach uwzględniających przedstawione powyżej czynniki. Aby określić liczbę taśm, należy wykonać następujące czynności:

1. Narysuj (lub zapisz) łańcuch kopii zapasowych, aż do momentu usunięcia pierwszej kopii zapasowej.
2. Uwzględnij opcje dołączania taśm, ponieważ łańcuch można podzielić na zestawy taśm.
3. Oblicz liczbę taśm dla każdego zestawu.
4. Suma obliczonych wartości będzie łączną liczbą taśm wymaganych w danym przypadku.

Planowanie taśm: Przykład 1

Przyjmijmy następujące założenia:

- Rozmiar pełnej kopii zapasowej wynosi **F_GB;**
- Średni rozmiar przyrostowych kopii zapasowych wynosi **I_GB;**
- Średni rozmiar różnicowych kopii zapasowych wynosi **D_GB;**
- Poziom kompresji zapewnia średni współczynnik redukcji **CL;**
- Wybrany schemat rotacji taśm to **Wieża Hanoi** z **czterema** poziomami;
- Ustawienia opcji dotyczących taśm są następujące:
  - Opcja **Użyj osobnego zestawu taśm** jest wybrana;
  - Opcja **Zawsze używaj wolnej taśmy: Do każdej pełnej kopii zapasowej** nie jest wybrana;
  - Opcja **Zawsze używaj wolnej taśmy: Do każdej przyrostowej kopii zapasowej** nie jest wybrana;
  - Opcja **Zawsze używaj wolnej taśmy: Dla każdej różnicowej kopii zapasowej** nie jest wybrana;
- Pojemność taśmy wynosi **T_GB**.

Schemat Wieża Hanoi z czterema poziomami (A, B, C i D) określa następującą kolejność tworzenia kopii zapasowych przed usunięciem pierwszej kopii zapasowej: D (pełna), A, B, A, C, A, B, A, D, A, B, A, C. Określone opcje dotyczące taśm nie wymagają używania wolnej taśmy dla żadnej kopii zapasowej, dlatego program automatycznie podzieli kopie i po osiągnięciu końca bieżącej taśmy będzie kontynuował ich zapisywanie na nowej taśmie. Należy obliczyć jeden zestaw taśm.

Łączna liczba wymaganych taśm = zaokrąglone w górę ((2*F_GB + 6*I_GB + 5*D_GB) * CL / T_GB) + 1.

Opisany powyżej Przykład 1 Wieży Hanoi (s. 171) używa pięciopoziomowego schematu tworzenia kopii zapasowych Wieża Hanoi z takimi samymi opcjami dotyczącymi taśm. Kolejność tworzenia kopii zapasowych jest następująca: E (pełna), A, B, A, C, A, B, A, D, A, B, A, C, A, B, A, E, A, B, A, C, A, B, A, D.

Łączna liczba wymaganych taśm = zaokrąglone w górę ((2*F_GB + 12*I_GB + 11*D_GB) * CL / T_GB) + 1 = zaokrąglone w górę ((2*320 + 12*16 + 11*40) * 1 / 400) + 1 = zaokrąglone w górę (3,18) + 1 = 5 (taśm).

Planowanie taśm: Przykład 2

Przyjmijmy następujące założenia:

- Rozmiar pełnej kopii zapasowej wynosi **F_GB;**
- Średni rozmiar przyrostowych kopii zapasowych wynosi **I_GB;**
- Średni rozmiar różnicowych kopii zapasowych wynosi **D_GB;**
- Poziom kompresji zapewnia średni współczynnik redukcji **CL;**
- Wybrano schemat rotacji taśm **Niestandardowa** z następującymi ustawieniami:
  - **pełna kopia zapasowa — co 10 dni;**
  - **różnicowa kopia zapasowa — co 2 dni;**
  - **przyrostowa kopia zapasowa — codziennie, co 6 godzin;**
  - **reguły przechowywania: usuwaj kopie zapasowe starsze niż 5 dni;**
- Ustawienia opcji dotyczących taśm są następujące:
  - Opcja **Użyj osobnego zestawu taśm** jest wybrana;
  - Opcja **Zawsze używaj wolnej taśmy: Do każdej pełnej kopii zapasowej** jest wybrana;
  - Opcja **Zawsze używaj wolnej taśmy: Do każdej przyrostowej kopii zapasowej** nie jest wybrana;
  - Opcja **Zawsze używaj wolnej taśmy: Dla każdej różnicowej kopii zapasowej** nie jest wybrana;
- Pojemność taśmy wynosi **T_GB**.

W tym przykładzie proces tworzenia kopii zapasowych składa się z dwóch sekcji. Poniższy rysunek prezentuje sekcje w chwili przed usunięciem pierwszej kopii zapasowej. Pełne, różnicowe i przyrostowe kopie zapasowe są oznaczone odpowiednio kolorami: pomarańczowym, niebieskim i zielonym.

Obecnie niektóre kopie zapasowe zostały usunięte przez zadanie Czyszczenie. Usunięcie przestarzałych kopii zapasowych oznaczonych ciemnym kolorem jest wstrzymane, ponieważ stanowią one podstawę dla aktualnych kopii zapasowych.

Ponieważ dokładny związek pomiędzy pojemnością taśmy a rozmiarem kopii zapasowej nie jest znany, nie można określić liczby taśm zwolnionych po usunięciu kopii. Dlatego w obliczeniach to prawdopodobieństwo jest pomijane.

W celu zapisania kopii zapasowych zestaw taśm 01 powinien zawierać (zaokrąglone w górę ((F_GB + 4*D_GB + 5*7*I_GB) * CL / T_GB)) taśm. W zestawie 02 należy użyć (zaokrąglone w górę ((F_GB + 1*D_GB + 7*I_GB) * CL / T_GB)) taśm. Suma obliczonych wartości określa łączną liczbę taśm wymaganych w tym przypadku.

Co zrobić

- **Co zrobić, aby przenieść taśmy z kopiami zapasowymi z jednej biblioteki taśm do drugiej?**

  1. Jeśli obie biblioteki taśm są podłączone do tego samego komputera, na którym jest zainstalowany węzeł magazynowania Acronis Backup & Recovery 10 Storage Node (np. biblioteki są zarządzane przez ten sam węzeł magazynowania), w bazie danych węzła magazynowania znajdują się wszystkie niezbędne informacje dotyczące zawartości przenoszonych taśm. Wystarczy zatem wykonać procedurę inwentaryzacji (s. 159) dla zarządzanego skarbca w bibliotece, w której umieszczono taśmy.
  2. Po przeniesieniu taśm do biblioteki zarządzanej przez inny węzeł magazynowania należy ponownie przeskanować (s. 159) wszystkie przeniesione taśmy w celu dodania do węzła magazynowania informacji na temat kopii zapasowych zapisanych na tych taśmach.

- **Co zrobić, aby użyć taśmy z biblioteki taśm w lokalnym urządzeniu taśmowym, lub odwrotnie: taśmy z urządzenia w bibliotece?**

  Agenty Acronis tworzą kopie zapasowe na taśmach w formacie różniącym się od formatu używanego przez węzeł magazynowania. Dlatego nie można zamieniać taśm pomiędzy urządzeniami taśmowymi podłączonymi do węzła magazynowania a podłączonymi do zarządzanego komputera: agent nie może odczytać taśmy zapisanej przez węzeł magazynowania w lokalnie podłączonym urządzeniu taśmowym. Jednak węzeł magazynowania może odczytać taśmy zapisane przez agenta. Pełne informacje na temat kompatybilności formatów taśm w programie Acronis Backup & Recovery 10 można znaleźć w tabeli kompatybilności taśm (s. 57).

- **Co zrobić, gdy trzeba zainstalować ponownie węzeł magazynowania lub podłączyć bibliotekę taśm do innego komputera?**

  Zainstaluj węzeł magazynowania na komputerze, do którego jest podłączona biblioteka taśm, utwórz skarbiec centralny w bibliotece taśm, a następnie przeskanuj ponownie wszystkie taśmy zawierające kopie zapasowe.

- **Co zrobić po utraceniu węzła magazynowania, aby odzyskać dane zapisane na taśmie?**

  Jeśli wiadomo, na której taśmie znajdują się dane do odzyskania i urządzenie taśmowe, na którym znajduje się skarbiec jest zarządzane przez węzeł magazynowania, włóż kasetę z taśmą do urządzenia, włącz w konsoli widok **Skarbce centralne**, wybierz skarbiec, przeskanuj ponownie taśmę, wybierz archiwum i kopię zapasową, z której chcesz odzyskać dane, a następnie utwórz zadanie odzyskiwania.

  Jeśli nie wiesz, na której taśmie znajdują się dane do odzyskania, musisz ponownie przeskanować wszystkie taśmy w celu znalezienia odpowiednich danych. Ogólnie wszystkie kroki, które należy wykonać, są takie same, jak opisane powyżej, z wyjątkiem ponownego skanowania wielu taśm zamiast jednej taśmy.

- **Co zrobić, aby odzyskać dane z taśmy Echo?**

  Informacje na temat możliwości odczytania danych z taśmy przez poszczególne komponenty Acronis Backup & Recovery 10 można znaleźć w sekcji Tabela kompatybilności taśm (s. 57).

4.2 Skarbce osobiste

Skarbiec osobisty to skarbiec utworzony przy użyciu bezpośredniego połączenia konsoli z komputerem zarządzanym. Skarbce osobiste są związane z konkretnym komputerem zarządzanym. Są one widoczne dla wszystkich użytkowników, którzy mogą zalogować się do systemu. Prawa użytkownika do tworzenia kopii zapasowych w skarbcu osobistym są zdefiniowane w jego uprawnieniach do folderu lub urządzenia, w którym znajduje się skarbiec.

Skarbiec osobisty może być przechowywany w udziale sieciowym, na serwerze FTP, na nośniku odłączanym lub wymiennym, w magazynie Acronis Online Backup Storage, w urządzeniu taśmowym

lub na lokalnym dysku twardym komputera. Strefa Acronis Secure Zone jest traktowana jako skarbiec osobisty dostępny dla wszystkich użytkowników, którzy mogą zalogować się do systemu. W przypadku tworzenia kopii zapasowych wymienionych wyżej lokalizacji skarbce osobiste są tworzone automatycznie.

Skarbce osobiste mogą być używane w lokalnych planach tworzenia kopii zapasowych i zadaniach lokalnych. Scentralizowane plany tworzenia kopii zapasowych nie korzystają ze skarbców osobistych, z wyjątkiem strefy Acronis Secure Zone.

Udostępnianie skarbca osobistego

Wiele komputerów może odnosić się do tej samej lokalizacji fizycznej, np. do tego samego udostępnionego folderu. Jednak każdy z komputerów ma swój własny skrót na drzewie **Skarbce**. Użytkownicy tworzący kopie zapasowe w folderze udostępnionym mogą wyświetlać archiwa innych użytkowników i zarządzać nimi zgodnie z posiadanymi uprawnieniami dostępu do danego folderu. W celu ułatwienia identyfikacji archiwów w widoku **Skarbiec osobisty** znajduje się kolumna **Właściciel** z informacjami o właścicielach poszczególnych archiwów. Aby dowiedzieć się więcej na temat pojęcia właściciela, zobacz Właściciele i poświadczenia (s. 35).

Metadane

Folder **.meta** jest tworzony w każdym skarbcu osobistym podczas tworzenia kopii zapasowej. Jest to folder zawierający dodatkowe informacje na temat archiwów i kopii zapasowych przechowywanych w skarbcu, w tym informacje o właścicielach archiwów i nazwach komputerów. W razie przypadkowego usunięcia folderu .meta zostanie on utworzony ponownie w sposób automatyczny przy kolejnym dostępie do skarbca. Jednak niektóre informacje, takie jak nazwy właścicieli i nazwy komputerów, mogą zostać utracone.

4.2.1 Praca z widokiem „Skarbiec osobisty”

W tej sekcji krótko opisano główne elementy widoku **Skarbiec osobisty** oraz przedstawiono sugestie dotyczące sposobu pracy z nim.

Pasek narzędzi skarbca

Pasek narzędzi zawiera przyciski operacyjne umożliwiające wykonanie operacji na wybranym skarbcu osobistym. Aby uzyskać szczegółowe informacje na ten temat, zobacz sekcję Czynności dotyczące skarbców osobistych (s. 179).

Wykres kołowy z legendą

Wykres kołowy umożliwia oszacowanie obciążenia skarbca. Przedstawia stosunek wolnego do zajętego miejsca w skarbcu.

— wolne miejsce: miejsce w urządzeniu pamięci, w którym znajduje się skarbiec. Jeśli na przykład skarbiec znajduje się na dysku twardym, wolnym miejscem skarbca jest wolne miejsce odpowiedniego woluminu.

— zajęte miejsce: łączny rozmiar archiwów kopii zapasowych i ich metadanych, o ile znajdują się w skarbcu. Inne pliki umieszczone w tym folderze przez użytkownika nie są uwzględniane.

Legenda zawiera następujące informacje o skarbcu:

- pełna ścieżka do skarbca;
- łączna liczba archiwów i kopii zapasowych przechowywanych w skarbcu;

- współczynnik zajętego miejsca do rozmiaru oryginalnych danych.

Zawartość skarbca

W sekcji **Zawartość skarbca** znajdują się tabela i pasek narzędzi archiwów. Tabela archiwów zawiera archiwa i kopie zapasowe przechowywane w skarbcu. Pasek narzędzi archiwów służy do wykonywania czynności na wybranych archiwach i kopiach zapasowych. Lista kopii zapasowych rozwija się po kliknięciu znaku „plus" z lewej strony nazwy archiwum. Wszystkie archiwa są pogrupowane według typów na następujących kartach:

- Na karcie **Archiwa dyskowe** znajduje się lista wszystkich archiwów zawierających kopie zapasowe (obrazy) dysków lub woluminów.
- Na karcie **Archiwa plikowe** znajduje się lista wszystkich archiwów zawierających kopie zapasowe plików.

Sekcje pokrewne:

Operacje na archiwach przechowywanych w skarbcu (s. 181)

Operacje na kopiach zapasowych (s. 182)

Filtrowanie i sortowanie archiwów (s. 183)

Paski na panelu „Czynności i narzędzia"

- **[Nazwa skarbca]** Pasek **Czynności** jest dostępny po kliknięciu skarbca w drzewie skarbców. Umożliwia wykonanie tych samych czynności, co pasek narzędzi skarbca.
- **[Nazwa archiwum]** Pasek **Czynności** jest dostępny po wybraniu archiwum w tabeli archiwów. Umożliwia wykonanie tych samych czynności, co pasek narzędzi archiwów.
- **[Nazwa kopii zapasowej]** Pasek **Czynności** jest dostępny po rozwinięciu archiwum i kliknięciu dowolnej z jego kopii zapasowych. Umożliwia wykonanie tych samych czynności, co pasek narzędzi archiwów.

4.2.2 Czynności dotyczące skarbców osobistych

Aby uzyskać dostęp do czynności

1. Podłącz konsolę do serwera zarządzania.
2. W panelu **Nawigacja** kliknij **Skarbce**> **Osobiste**.

Wszystkie opisane tutaj operacje wykonuje się przez kliknięcie odpowiednich przycisków na pasku narzędzi skarbców. Dostęp do tych operacji można również uzyskać, wybierając element **Czynności [nazwa skarbca]** w menu głównym.

Poniżej przedstawiono wskazówki dotyczące wykonywania operacji na skarbcach osobistych.

Zadanie	Czynności
Tworzenie skarbca osobistego	Kliknij **Utwórz**. Procedura tworzenia skarbców osobistych jest szczegółowo opisana w sekcji Tworzenie skarbca osobistego (s. 180).
Edycja skarbca	1. Wybierz skarbiec. 2. Kliknij **Edytuj**. Na stronie **Edytuj skarbiec osobisty** można zmienić nazwę skarbca i informacje w polu **Komentarze**.

Zmiana konta użytkownika umożliwiającego dostęp do skarbca	Kliknij **Zmień użytkownika**. W wyświetlonym oknie dialogowym podaj poświadczenia wymagane do uzyskania dostępu do skarbca.
Tworzenie strefy Acronis Secure Zone	Kliknij **Utwórz strefę Acronis Secure Zone**. Procedura tworzenia strefy Acronis Secure Zone jest szczegółowo opisana w sekcji Tworzenie strefy Acronis Secure Zone (s. 286).
Eksplorowanie zawartości skarbca	Kliknij **Eksploruj**. W wyświetlonym oknie Eksploratora przejrzyj zawartość wybranego skarbca.
Sprawdzanie poprawności skarbca	Kliknij **Sprawdź poprawność**. Nastąpi przejście do strony Sprawdzanie poprawności (s. 271), na której ten skarbiec będzie wstępnie wybrany jako źródło. Sprawdzenie poprawności skarbca polega na sprawdzeniu wszystkich archiwów przechowywanych w tym skarbcu.
Usuwanie skarbca	Kliknij **Usuń**. Operacja usunięcia w rzeczywistości powoduje tylko usunięcie skrótu do danego folderu z widoku **Skarbce**. Sam folder pozostaje niezmieniony. Archiwa znajdujące się w folderze można zachować lub usunąć.
Odświeżanie informacji w tabeli skarbców	Kliknij **Odśwież**. Podczas przeglądania zawartości skarbca można dodawać, usuwać i modyfikować jego archiwa. Kliknij **Odśwież**, aby w informacjach dotyczących skarbca uwzględnić najnowsze zmiany.

Tworzenie skarbca osobistego

Aby utworzyć skarbiec osobisty

1. W polu **Nazwa** wpisz nazwę tworzonego skarbca.
2. [Opcjonalnie] W polu **Komentarze** dodaj opis skarbca.
3. W polu **Ścieżka** kliknij **Zmień**.
   W otwartym oknie **Ścieżka skarbca osobistego** określ ścieżkę do folderu, który będzie służyć jako skarbiec. Skarbiec osobisty można zorganizować na odłączanym lub wymiennym nośniku, udziale sieciowym lub serwerze FTP.
4. Kliknij **OK**. W efekcie utworzony skarbiec pojawi się w grupie **Osobiste** w drzewie skarbców.

Scalanie i przenoszenie skarbców osobistych

Co należy zrobić, aby przenieść istniejący skarbiec z jednego miejsca do innego?

Wykonaj następujące czynności

1. Przenosząc pliki, upewnij się, że z istniejącego skarbca nie korzysta żaden z planów tworzenia kopii zapasowych. Ewentualnie tymczasowo wyłącz (s. 213) harmonogramy danych planów.
2. Ręcznie przenieś folder skarbca ze wszystkimi jego archiwami do nowego miejsca przy użyciu menedżera plików innej firmy.
3. Utwórz nowy skarbiec.
4. Edytuj plany i zadania tworzenia kopii zapasowych: przekieruj ich miejsce docelowe do nowego skarbca.
5. Usuń stary skarbiec.

W jaki sposób można scalić dwa skarbce?

Przypuśćmy, że istnieją dwa skarbce *A* i *B*. Oba są używane w planach tworzenia kopii zapasowych. Decydujesz się pozostawić jedynie skarbiec *B*, przenosząc do niego wszystkie archiwa ze skarbca *A*.

W tym celu wykonaj następujące czynności

1. Scalając skarbce, upewnij się, że ze skarbca *A* nie korzysta żaden z planów tworzenia kopii zapasowych. Ewentualnie tymczasowo wyłącz (s. 213) harmonogramy danych planów.
2. Ręcznie przenieś archiwa do skarbca *B* przy użyciu menedżera plików innej firmy.
3. Edytuj plany tworzenia kopii zapasowych korzystające ze skarbca *A*: przekieruj ich miejsce docelowe do skarbca *B*.
4. W drzewie skarbców zaznacz skarbiec *B*, aby sprawdzić, czy zostaną wyświetlone archiwa. Jeśli tak nie jest, kliknij **Odśwież**.
5. Usuń skarbiec *A*.

4.3 Typowe operacje

4.3.1 Operacje na archiwach przechowywanych w skarbcu

Aby wykonać jakąkolwiek operację na archiwum, należy je najpierw zaznaczyć. Jeśli archiwum jest chronione hasłem, pojawi się monit o jego podanie.

Wszystkie operacje opisane poniżej wykonuje się przez kliknięcie odpowiednich przycisków na pasku narzędzi. Dostęp do tych operacji można również uzyskać na pasku **Czynności [nazwa archiwum]** (w panelu **Czynności i narzędzia**) oraz za pomocą pozycji **Czynności [nazwa archiwum]** w menu głównym.

Poniżej przedstawiono wskazówki dotyczące wykonywania operacji na archiwach przechowywanych w skarbcu.

Zadanie	Czynności
Sprawdzanie poprawności archiwum	Kliknij **Sprawdź poprawność**. Zostanie otwarta strona **Sprawdzanie poprawności (s. 271)** ze wstępnie wybranym archiwum jako źródłem. Sprawdzenie poprawności archiwum oznacza sprawdzenie wszystkich kopii zapasowych w tym archiwum.
Eksportowanie archiwum	Kliknij **Eksport**. Zostanie otwarta strona **Eksport** (s. 279) ze wstępnie wybranym archiwum jako źródłem. Eksport archiwum polega na utworzeniu w wybranej lokalizacji kopii archiwum ze wszystkimi kopiami zapasowymi.
Usuwanie pojedynczego archiwum lub wielu archiwów	1. Wybierz archiwum lub jedno z archiwów do usunięcia. 2. Kliknij **Usuń**. Program przedstawi dokonany wybór w oknie **Usuwanie kopii zapasowej** (s. 183), które zawiera pola wyboru obok każdego archiwum i każdej kopii zapasowej. Przejrzyj i w razie potrzeby zmień wybór (zaznacz pola wyboru żądanych archiwów), a następnie potwierdź usunięcie.
Usuwanie wszystkich archiwów ze skarbca	Należy pamiętać, że jeśli na liście skarbców zastosowano filtry, jest widoczna tylko część zawartości skarbca. Przed rozpoczęciem operacji upewnij się, że skarbiec nie

	zawiera żadnych potrzebnych archiwów. Kliknij **Usuń wszystkie**. Program przedstawi dokonany wybór w nowym oknie, które zawiera pola wyboru obok każdego archiwum i każdej kopii zapasowej. Przejrzyj i w razie potrzeby zmień wybór, a następnie potwierdź usunięcie.

4.3.2 Operacje na kopiach zapasowych

Aby wykonać jakąkolwiek operację na kopii zapasowej, kopię należy najpierw zaznaczyć. Aby zaznaczyć kopię zapasową, rozwiń archiwum, a następnie kliknij kopię zapasową. Jeśli archiwum jest chronione hasłem, pojawi się monit o jego podanie.

Wszystkie operacje opisane poniżej wykonuje się przez kliknięcie odpowiednich przycisków na pasku narzędzi. Dostęp do tych operacji można również uzyskać na **pasku Czynności „[nazwa kopii zapasowej]”** (w panelu **Czynności i narzędzia**) oraz za pomocą pozycji **Czynności „[nazwa kopii zapasowej]”** w menu głównym.

Poniżej przedstawiono wskazówki dotyczące wykonywania operacji na kopiach zapasowych.

Zadanie	Czynności
Wyświetlanie zawartości kopii zapasowej w oddzielnym oknie	Kliknij **Wyświetl zawartość**. W oknie **Zawartość kopii zapasowej** sprawdź zawartość kopii zapasowej.
Odzyskaj	Kliknij **Odzyskaj**. Zostanie otwarta strona **Odzyskaj dane** ze wstępnie wybraną kopią zapasową jako źródłem.
Odzyskiwanie dysku/woluminu jako maszyny wirtualnej	Kliknij prawym przyciskiem myszy kopię zapasową dysku, a następnie wybierz **Odzyskaj jako maszynę wirtualną**. Zostanie otwarta strona **Odzyskaj dane** ze wstępnie wybraną kopią zapasową jako źródłem. Wybierz lokalizację i typ nowej maszyny wirtualnej, a następnie wykonaj zwykłe czynności jak przy odzyskiwaniu zwykłego dysku lub woluminu.
Sprawdzanie poprawności kopii zapasowej	Kliknij **Sprawdź poprawność**. Zostanie otwarta strona **Sprawdzanie poprawności (s. 271)** ze wstępnie wybraną kopią zapasową jako źródłem. Sprawdzanie poprawności kopii zapasowej plików jest operacją symulującą odzyskiwanie wszystkich plików z kopii zapasowej do tymczasowego miejsca docelowego. Sprawdzanie poprawności kopii zapasowej dysku polega na obliczeniu sumy kontrolnej każdego bloku danych zapisanego w kopii zapasowej.
Eksportowanie kopii zapasowej	Kliknij **Eksport**. Zostanie otwarta strona **Eksport** (s. 279) ze wstępnie wybraną kopią zapasową jako źródłem. Eksport kopii zapasowej polega na utworzeniu w wybranej lokalizacji nowego archiwum z samowystarczalną kopią zapasową.
Usuwanie jednej lub wielu kopii zapasowych	Wybierz jedną z kopii zapasowych do usunięcia, a następnie kliknij **Usuń**. Program przedstawi dokonany wybór w oknie **Usuwanie kopii zapasowej** (s. 183), które zawiera pola wyboru obok każdego archiwum i każdej kopii zapasowej. Przejrzyj i w razie potrzeby zmień wybór (zaznacz pola wyboru żądanych kopii zapasowych), a następnie potwierdź usunięcie.

Usuwanie wszystkich archiwów i kopii zapasowych ze skarbca	Należy pamiętać, że jeśli na liście skarbców zastosowano filtry, jest widoczna tylko część zawartości skarbca. Przed rozpoczęciem operacji upewnij się, że skarbiec nie zawiera żadnych potrzebnych archiwów. Kliknij **Usuń wszystkie**. Program przedstawi dokonany wybór w oknie **Usuwanie kopii zapasowej** (s. 183), które zawiera pola wyboru obok każdego archiwum i każdej kopii zapasowej. Przejrzyj i w razie potrzeby zmień wybór, a następnie potwierdź usunięcie.

4.3.3 Usuwanie archiwów i kopii zapasowych

W oknie **Backups deletion** (Usunięcie kopii zapasowych) jest wyświetlana taka sama karta, jak w widoku skarbców, ale z polami wyboru obok każdego archiwum i każdej kopii zapasowej. Obok archiwum lub kopii zapasowej do usunięcia znajduje się znacznik wyboru. Przejrzyj archiwa i kopie zapasowe wybrane do usunięcia. Aby usunąć inne archiwa i kopie zapasowe, zaznacz odpowiednie pola wyboru, a następnie kliknij **Usuń wybrane** i potwierdź usunięcie.

Filtry w tym oknie pochodzą z listy archiwów w widoku skarbca. Dlatego jeśli na liście archiwów zastosowano jakieś filtry, zostaną tutaj wyświetlone tylko archiwa i kopie zapasowe spełniające kryteria tych filtrów. Aby wyświetlić całą zawartość, należy wyczyścić wszystkie pola filtrów.

Co się stanie, jeśli usunę kopię zapasową, która jest podstawą do tworzenia przyrostowej lub różnicowej kopii zapasowej?

Aby zachować spójność archiwów, program skonsoliduje dwie kopie zapasowe. Załóżmy na przykład, że trzeba usunąć pełną kopię zapasową, ale zachować kolejną kopię przyrostową. Kopie zapasowe zostaną scalone w jedną pełną kopię zapasową, której datą utworzenia będzie data utworzenia przyrostowej kopii zapasowej. Po usunięciu przyrostowej lub różnicowej kopii zapasowej ze środka łańcucha wynikową kopią zapasową będzie kopia przyrostowa.

Należy pamiętać, że konsolidacja to jedynie metoda usuwania, ale nie alternatywa do usuwania. Wynikowa kopia zapasowa nie będzie zawierać danych, które były obecne w usuniętej kopii zapasowej i których nie było w zachowanej przyrostowej lub różnicowej kopii zapasowej.

W skarbcu należy zapewnić wystarczającą ilość wolnego miejsca na pliki tymczasowe tworzone podczas konsolidacji. Wynikowe kopie zapasowe z konsolidacji zawsze mają maksymalną kompresję.

4.3.4 Filtrowanie i sortowanie archiwów

Poniżej przedstawiono wytyczne dotyczące filtrowania i sortowania archiwów w tabeli archiwów.

Zadanie	Działanie
Sortuj archiwa kopii zapasowych według dowolnej kolumny	Kliknij nagłówek kolumny, aby posortować archiwa w porządku rosnącym. Kliknij ponownie nagłówek kolumny, aby posortować archiwa w porządku malejącym.
Filtruj archiwa według nazwy, właściciela lub komputera	W polu pod odpowiednim nagłówkiem kolumny wpisz nazwę archiwum (nazwę właściciela lub nazwę komputera). Zostanie wyświetlona lista archiwów, których nazwy (lub nazwy właścicieli albo nazwy komputerów) są w pełni lub częściowo zgodne z wprowadzoną wartością.

Konfigurowanie tabeli archiwów

Domyślnie w tabeli jest wyświetlanych siedem kolumn, a pozostałe są ukryte. W razie potrzeby można ukryć wyświetlane kolumny i wyświetlić kolumny ukryte.

Aby wyświetlić lub ukryć kolumny

1. Kliknij prawym przyciskiem myszy nagłówek kolumny, aby wyświetlić menu kontekstowe. Zaznaczone elementy menu odpowiadają nagłówkom kolumn wyświetlanych w tabeli.
2. Kliknij elementy, które chcesz wyświetlić/ukryć.

5 Tworzenie harmonogramu

Funkcja harmonogramu dostępna w oprogramowaniu Acronis umożliwia administratorowi dostosowanie planów tworzenia kopii zapasowych do codziennego cyklu funkcjonowania firmy i stylu pracy każdego pracownika. Zadania planu są wykonywane systematycznie, a krytyczne dane skutecznie chronione.

Funkcja harmonogramu wykorzystuje lokalny czas komputera, na którym znajduje się plan tworzenia kopii zapasowych. Przed utworzeniem harmonogramu należy się upewnić, że ustawienia daty i godziny komputera są poprawne.

Harmonogram

Aby zdefiniować czas wykonywania zadania, należy określić jedno lub więcej zdarzeń. Zadanie zostanie uruchomione bezpośrednio po wystąpieniu jednego ze zdarzeń. W poniższej tabeli znajduje się lista zdarzeń dostępnych w systemach operacyjnych Windows i Linux.

Zdarzenie	Windows	Linux
Czas: Codziennie, Co tydzień, Co miesiąc	+	+
Czas, jaki upłynął od ostatniego pomyślnego utworzenia kopii zapasowej (można określić czas)	+	+
Logowanie użytkownika (dowolny użytkownik, bieżący użytkownik, określone konto użytkownika)	+	-
Wylogowanie użytkownika* (dowolny użytkownik, bieżący użytkownik, określone konto użytkownika) *Zamknięcie systemu nie jest tożsame z wylogowaniem użytkownika. Zadanie nie zostanie uruchomione przy zamknięciu systemu.	+	-
Uruchamianie systemu	+	+
Zmiana ilości wolnego miejsca (można określić wielkość zmiany ilości wolnego miejsca na dowolnym woluminie wybranym do tworzenia kopii zapasowej lub zawierającym dane przeznaczone do kopii zapasowej)	+	-
Zdarzenie w dzienniku zdarzeń systemu Windows (można określić parametry zdarzenia)	+	-
W przypadku alertu programu Acronis Drive Monitor	+	-

Warunek

W przypadku operacji tworzenia kopii zapasowych (i tylko takich operacji) oprócz zdarzeń można określić jeden lub więcej warunków. Po wystąpieniu dowolnego ze zdarzeń funkcja harmonogramu sprawdza warunek i w przypadku jego spełnienia uruchamia zadanie. W przypadku wielu warunków wszystkie z nich muszą być spełnione jednocześnie, aby program uruchomił zadanie. W poniższej tabeli znajduje się lista warunków dostępnych w systemach operacyjnych Windows i Linux.

Warunek: uruchom zadanie tylko jeśli...	Windows	Linux
Użytkownik jest bezczynny (uruchomiony jest wygaszacz ekranu lub komputer jest zablokowany)	+	-

Host lokalizacji jest dostępny	+	+
Czas wykonania zadania mieści się w określonym przedziale czasowym	+	+
Wszyscy użytkownicy są wylogowani	+	-
Minął określony czas od ostatniego pomyślnego utworzenia kopii zapasowej	+	+

Gdy wystąpi zdarzenie, a warunek (lub jeden z wielu warunków) nie zostanie spełniony, działanie funkcji harmonogramu określa opcja tworzenia kopii zapasowych Warunki uruchomienia zadania (s. 129).

Co się wydarzy, jeśli...

- **Co się wydarzy, jeśli zdarzenie wystąpi (a ewentualny warunek zostanie spełniony) w momencie, gdy wykonywanie poprzedniego zadania nie zostało zakończone?**

  Zdarzenie zostanie zignorowane.
- **Co się wydarzy, jeśli zdarzenie wystąpi w momencie, gdy funkcja harmonogramu oczekuje na spełnienie warunku wymaganego przez poprzednie zdarzenie?**

  Zdarzenie zostanie zignorowane.
- **Co się wydarzy, jeśli warunek pozostanie niespełniony przez bardzo długi czas?**

  Jeżeli opóźnienie tworzenia kopii zapasowej staje się ryzykowne, można wymusić dany warunek (nakazać użytkownikom wylogowanie) lub uruchomić zadanie ręcznie. Aby zapewnić automatyczne postępowanie w takiej sytuacji, można ustawić czas, po upływie którego zadanie zostanie uruchomione niezależnie od spełnienia warunku.

5.1 Harmonogram dzienny

Harmonogram dzienny jest dostępny w systemach operacyjnych Windows i Linux.

Aby określić harmonogram dzienny

W obszarze **Harmonogram** zaznacz właściwy parametr w następujący sposób:

Co: <...> dzień/dni	Wyznacz częstotliwość wykonywania zadania. Jeżeli na przykład wybierzesz co 2 dni, zadanie będzie uruchamiane co drugi dzień.

W obszarze **Wykonaj zadanie w ciągu dnia** zaznacz jedną z następujących opcji:

Raz o: <...>	Wyznacz godzinę jednokrotnego wykonania zadania.
Co: <...> **Od: <...>** **do: <...>**	Wyznacz, ile razy zadanie będzie wykonywane w określonym przedziale czasowym. Wyznaczenie częstotliwości zadania np. co godzinę od 10:00:00 do 22:00:00 umożliwia wykonanie zadania 12 razy jednego dnia: od 10 rano do 10 wieczorem.

W obszarze **Obowiązuje** określ następujące ustawienia:

Od: <...>	Wyznacz początkową datę obowiązywania harmonogramu (data rozpoczęcia obowiązywania). Jeżeli to pole wyboru nie jest zaznaczone, zadanie zostanie uruchomione najbliższego dnia o godzinie określonej powyżej.
Do: <...>	Wyznacz końcową datę obowiązywania harmonogramu. Jeżeli to pole wyboru nie jest zaznaczone, zadanie będzie uruchamiane przez nieskończoną liczbę dni.

Ustawienia zaawansowane harmonogramu (s. 195) są dostępne tylko w komputerach zarejestrowanych na serwerze Acronis Backup & Recovery 10 Management Server. Aby określić te ustawienia, kliknij **Zmień** w obszarze **Ustawienia zaawansowane**.

Wszystkie wybrane ustawienia są wyświetlane w polu **Wynik** na dole okna.

Przykłady

„Prosty" harmonogram dzienny

Uruchom zadanie codziennie o 18.00.

Parametry harmonogramu są następujące:

1. Co: **1** dzień.
2. Raz o: **18:00:00**.
3. Obowiązuje:

   Od: **nie ustawiono**. Zadanie zostanie uruchomione w bieżącym dniu, jeżeli zostało utworzone przed 18.00. Zadanie utworzone po 18.00 zostanie uruchomione po raz pierwszy następnego dnia o tej porze.

   Do: **nie ustawiono**. Zadanie będzie wykonywanie przez nieskończoną liczbę dni.

Harmonogram „Trzygodzinny interwał czasu przez trzy miesiące"

Uruchom zadanie co trzy godziny. Zadanie rozpoczyna się w danym dniu (np. 15 września 2009 r.) i kończy po trzech miesiącach.

Parametry harmonogramu są następujące:

1. Co: **1** dzień.
2. Co: **3** godziny.

   Od: **12:00:00** (północ) Do: **21:00:00** — tak więc zadanie zostanie wykonane 8 razy dziennie z 3 godzinną przerwą. Po ostatnim dziennym powtórzeniu o 21.00, nadchodzi następny dzień i zadanie rozpoczyna się ponownie od północy.
3. Obowiązuje:

   Od: **15 września 2009**. Jeżeli zadanie zostało utworzone 15 września 2009 r. o 13.15, jego wykonanie rozpocznie się po nadejściu najwcześniejszego interwału czasowego: w naszym przykładzie o 15.00.

   Do: **15 grudnia 2009**. W tym dniu zadanie zostanie wykonane po raz ostatni, ale będzie ono nadal dostępne w widoku **Zadania**.

Kilka harmonogramów dziennych dla jednego zadania

Są sytuacje, kiedy zadanie trzeba uruchomić kilka razy dziennie, a nawet kilka razy dziennie z różnymi interwałami czasowymi. W takich przypadkach można rozważyć przypisanie kilku harmonogramów do jednego zadania.

Załóżmy na przykład, że zadanie trzeba wykonać co trzeci dzień, zaczynając od 20 września 2009 r., pięć razy dziennie:

- pierwszy raz o 8.00,
- drugi raz o 12.00 (południe),
- trzeci raz o 15.00,
- czwarty raz o 17.00,
- piąty raz o 19.00.

Najbardziej oczywistym rozwiązaniem jest dodanie pięciu prostych harmonogramów. Po nieco dłuższym zastanowieniu można znaleźć bardziej optymalną metodę. Jak widać, interwał czasowy pomiędzy pierwszym a drugim wykonaniem zadania wynosi 4 godziny, a pomiędzy trzecim, czwartym

i piątym 2 godziny. W takim przypadku optymalne będzie przypisanie dwóch harmonogramów do zadania.

Pierwszy harmonogram dzienny

1. Co: **3** dni.
2. Co: **4** godziny.
   Od: **08:00:00** Do: **12:00:00**.
3. Obowiązuje:
   Od: **20 września 2009**.
   Do: **nie ustawiono**.

Drugi harmonogram dzienny

1. Co: **3** dni.
2. Co: **2** godziny.
   Od: **15:00:00** Do: **19:00:00**.
3. Obowiązuje:
   Od: **20 września 2009**.
   Do: **nie ustawiono**.

5.2 Harmonogram tygodniowy

Harmonogram tygodniowy jest dostępny w systemach operacyjnych Windows i Linux.

Aby określić harmonogram tygodniowy

W obszarze **Harmonogram** zaznacz właściwy parametr w następujący sposób:

Co: <...> tygodni w dniu: <...>	Określ liczbę tygodni oraz poszczególne dni tygodnia, kiedy zadanie będzie uruchamiane. Przy ustawieniu np. co **2** tygodnie w **Pon** zadanie będzie wykonywane co drugi tydzień w poniedziałek.

W obszarze **Wykonaj zadanie w ciągu dnia** zaznacz jedną z następujących opcji:

Raz o: <...>	Wyznacz godzinę jednokrotnego wykonania zadania.
Co: <...> **Od: <...> do: <...>**	Wyznacz, ile razy zadanie będzie wykonywane w określonym przedziale czasowym. Wyznaczenie częstotliwości zadania na przykład na co **1** godzinę od **10:00:00** do **22:00:00** umożliwia wykonanie zadania 12 razy jednego dnia: od 10 rano do 10 wieczorem.

W obszarze **Obowiązuje** określ następujące ustawienia:

Od: <...>	Wyznacz początkową datę obowiązywania harmonogramu (data rozpoczęcia obowiązywania). Jeżeli to pole wyboru nie jest zaznaczone, zadanie zostanie uruchomione najbliższego dnia o godzinie określonej powyżej.
Do: <...>	Wyznacz końcową datę obowiązywania harmonogramu. Jeżeli to pole wyboru nie jest zaznaczone, zadanie będzie uruchamiane przez nieskończoną liczbę tygodni.

Ustawienia zaawansowane harmonogramu (s. 195) są dostępne tylko w komputerach zarejestrowanych na serwerze Acronis Backup & Recovery 10 Management Server. Aby określić te ustawienia, kliknij **Zmień** w obszarze **Ustawienia zaawansowane**.

Wszystkie wybrane ustawienia są wyświetlane w polu **Wynik** na dole okna.

Przykłady

Harmonogram „Jeden dzień w tygodniu”

Uruchom zadanie w każdy piątek o 22.00 od określonego dnia (np. 14 maja 2009 r.) przez sześć miesięcy.

Parametry harmonogramu są następujące:

1. Co: **1** tydzień w: **Pią**.
2. Raz o: **22:00:00**.
3. Obowiązuje:

   Od: **13 maja 2009**. Zadanie zostanie uruchomione w najbliższy piątek o 22.00.

   Do: **13 listopada 2009**. W tym dniu zadanie zostanie wykonane po raz ostatni, ale po tej dacie będzie nadal dostępne w widoku Zadania (gdy data nie wypada w piątek, zadanie zostanie wykonane po raz ostatni w ostatni piątek poprzedzający tę datę).

Ten harmonogram jest powszechnie wykorzystywany przy niestandardowym schemacie tworzenia kopii zapasowych. Harmonogram typu „Jeden dzień w tygodniu” przypisuje się do pełnych kopii zapasowych, podczas gdy przyrostowe kopie bezpieczeństwa są zaplanowane w dni robocze. Szczegółowe informacje można znaleźć w przykładzie „Pełne i przyrostowe kopie zapasowe plus czyszczenie” w sekcji Schemat niestandardowy tworzenia kopii zapasowych (s. 243).

Harmonogram „W dni robocze”

Uruchom zadanie w każdym tygodniu w dni robocze: od poniedziałku do piątku. W dniu roboczym zadanie jest uruchamiane tylko raz o 21.00.

Parametry harmonogramu są następujące:

1. Co: **1** tydzień w: **<Dni robocze>** — po zaznaczeniu pola wyboru <Dni robocze> następuje automatyczne zaznaczenie odpowiednich pól (**Pon**, **Wto**, **Śro**, **Czw** i **Pią**), podczas gdy inne pola pozostają bez zmian.
2. Raz o: **21:00:00**.
3. Obowiązuje:

   Od: **puste**. Po utworzeniu zadania — np. w poniedziałek o 11.30 — zostanie ono uruchomione tego samego dnia o 21.00. Gdy zadanie utworzymy np. w piątek po 21.00, wówczas zostanie ono uruchomione po raz pierwszy w najbliższym dniu roboczym (w naszym przykładzie w poniedziałek) o 21.00.

   Data końcowa: **puste**. Zadanie będzie wykonywane przez nieskończoną liczbę tygodni.

Ten harmonogram jest powszechnie wykorzystywany przy niestandardowym schemacie tworzenia kopii zapasowych. Harmonogram typu „W dni robocze” przypisuje się do przyrostowych kopii zapasowych, podczas gdy wykonywanie pełnej kopii zapasowej jest zaplanowane raz w tygodniu. Szczegółowe informacje można znaleźć w przykładzie „Pełne i przyrostowe kopie zapasowe plus czyszczenie” w sekcji Schemat niestandardowy tworzenia kopii zapasowych (s. 243).

Kilka harmonogramów tygodniowych dla jednego zadania

Jeżeli trzeba wykonać zadanie w różne dni tygodnia z różnymi interwałami czasowymi, rozważ przypisanie specjalnego harmonogramu do każdego pożądanego dnia tygodnia lub do kilku dni.

Jeżeli na przykład zadanie ma być uruchamiane zgodnie z następującym harmonogramem:

- Poniedziałek: dwa razy — o 12.00 (południe) i 21.00

- Wtorek: co trzy godziny od 9.00 do 21.00
- Środa: co trzy godziny od 9.00 do 21.00
- Czwartek: co trzy godziny od 9.00 do 21.00
- Piątek: dwa razy — o 12.00 (południe) i 21.00 (tak samo jak w poniedziałek)
- Sobota: raz o 21.00
- Niedziela: raz o 21.00

Po połączeniu identycznych pór trzy następujące harmonogramy można przypisać do zadania:

Pierwszy harmonogram

1. Co: **1** tydzień w: **Pon**, **Pią**.
2. Co: **9** godzin.
   Od: **12:00:00** Do: **21:00:00**.
3. Obowiązuje:
   Od: **nie ustawiono**.
   Do: **nie ustawiono**.

Drugi harmonogram

1. Co **1** tydzień w: **Wto**, **Śro**, **Czw**.
2. Co: **3** godziny.
   Od: **09:00:00** do: **21:00:00**.
3. Obowiązuje:
   Od: **nie ustawiono**.
   Do: **nie ustawiono**.

Harmonogram trzeci

1. Co: **1** tydzień w: **Sob, Nie**.
2. Raz o: **21:00:00**.
3. Obowiązuje:
   Od: **nie ustawiono**.
   Do: **nie ustawiono**.

5.3 Harmonogram miesięczny

Harmonogram miesięczny jest dostępny w systemach operacyjnych Windows i Linux.

Aby określić harmonogram miesięczny

W obszarze **Harmonogram** zaznacz właściwy parametr w następujący sposób:

Miesiące: <...>	Wybierz miesiąc lub miesiące, kiedy zadanie ma być wykonywane.
Dni: <...>	Wybierz konkretne dni miesiąca, kiedy zadanie będzie wykonywane. Możesz również wybrać ostatni dzień miesiąca — niezależnie od jego faktycznej daty.
W: <...>	Wybierz konkretne dni tygodnia, kiedy zadanie ma być wykonywane.

W obszarze **Wykonaj zadanie w ciągu dnia** zaznacz jedno z następujących:

Raz o: <...>	Wyznacz godzinę jednokrotnego wykonania zadania.
Co: <...> **Od: <...>** **do: <...>**	Wyznacz, ile razy zadanie będzie wykonywane w określonym przedziale czasowym. Wyznaczenie częstotliwości zadania na przykład na co **1** godzinę od **10:00:00** do **22:00:00** umożliwia wykonanie zadania 12 razy jednego dnia: od 10 rano do 10 wieczorem.

W obszarze **Obowiązuje** określ następujące ustawienia:

Od: <...>	Wyznacz początkową datę obowiązywania harmonogramu (data rozpoczęcia obowiązywania). Jeżeli to pole wyboru nie jest zaznaczone, zadanie zostanie uruchomione najbliższego dnia o godzinie określonej powyżej.
Do: <...>	Wyznacz końcową datę obowiązywania harmonogramu. Jeżeli to pole wyboru nie jest zaznaczone, zadanie będzie uruchamiane przez nieskończoną liczbę miesięcy.

Ustawienia zaawansowane harmonogramu (s. 195) są dostępne tylko w komputerach zarejestrowanych na serwerze Acronis Backup & Recovery 10 Management Server. Aby określić te ustawienia, kliknij **Zmień** w obszarze **Ustawienia zaawansowane**.

Wszystkie wybrane ustawienia są wyświetlane w polu **Wynik** na dole okna.

Przykłady

Harmonogram „Ostatni dzień każdego miesiąca”

Uruchom zadanie raz o 22.00 w ostatnim dniu każdego miesiąca.

Parametry harmonogramu są następujące:

1. Miesiące: **<Wszystkie miesiące>**.
2. Dni: **Ostatni**. Zadanie będzie wykonywane w ostatnim dniu każdego miesiąca — niezależnie od faktycznej daty.
3. Raz o: **22:00:00**.
4. Obowiązuje:

   Od: **puste**.

   Do: **puste**.

Ten harmonogram jest powszechnie wykorzystywany przy niestandardowym schemacie tworzenia kopii zapasowych. Harmonogram typu „Ostatni dzień miesiąca” przypisuje się do pełnych kopii zapasowych, podczas gdy wykonywanie różnicowych kopii bezpieczeństwa jest zaplanowane jeden raz w tygodniu, a przyrostowych — w dni robocze. Szczegółowe informacje można znaleźć w przykładzie „Pełne miesięczne, tygodniowe różnicowe i dzienne przyrostowe kopie zapasowe plus czyszczenie” w sekcji Schemat niestandardowy tworzenia kopii zapasowych (s. 243).

Harmonogram „Pora roku”

Uruchom zadanie we wszystkie dni jesieni na półkuli północnej w roku 2009 i 2010. W dniu roboczym zadanie będzie wykonywane co 6 godzin od 24.00 do 18.00.

Parametry harmonogramu są następujące:

1. Miesiące: **wrzesień, październik, listopad**.
2. W: **<wszystkie> <dni robocze>**.
3. Co: **6** godzin.

Od: **24:00:00** Do: **18:00:00**.

4. Obowiązuje:

   Od: **30 sierpnia 2009**. Zadanie faktycznie zostanie uruchomione w pierwszym dniu września. Określając tę datę, po prostu ustalamy, że zadanie musi być uruchomione w 2009 roku.

   Do: **1 grudnia 2010**. Zadanie faktycznie zakończy się w ostatnim dniu roboczym listopada. Określając tę datę, po prostu ustalamy, że zadanie musi zakończyć się w 2010 roku — po upływie jesieni na półkuli północnej.

Kilka harmonogramów miesięcznych dla jednego zadania

Jeżeli zadanie trzeba wykonać w różne dni lub w różne tygodnie z różnymi interwałami czasowymi w zależności od miesiąca, rozważ przypisanie specjalnego harmonogramu do każdego pożądanego miesiąca lub do kilku miesięcy.

Załóżmy, że zadanie zacznie obowiązywać od 1 listopada 2009 r.

- Podczas zimy na półkuli północnej zadanie jest uruchamiane jeden raz o 22.00 w każdy dzień roboczy.
- Podczas wiosny i jesieni na półkuli północnej zadanie jest uruchamiane co 12 godzin we wszystkie dni robocze.
- Podczas lata na półkuli północnej zadanie jest uruchamiane w każdy pierwszy i piętnasty dzień każdego miesiąca o 22.00.

W ten sposób do zadania przypisane zostały trzy następujące harmonogramy:

Pierwszy harmonogram

1. Miesiące: **grudzień**, **styczeń**, **luty**.
2. W: **<Wszystkie> <Dni robocze>**.
3. Raz o: **22:00:00**.
4. Obowiązuje:

   Od: **1 listopada 2009**.

   Do: **nie ustawiono**.

Drugi harmonogram

1. Miesiące: **marzec**, **kwiecień**, **maj**, **wrzesień**, **październik**, **listopad**.
2. W: **<Wszystkie> <Dni robocze>**.
3. Co: **12 godzin**

   Od: **24:00:00** Do: **12:00:00**.
4. Obowiązuje:

   Od: **1 listopada 2009**.

   Do: **nie ustawiono**.

Harmonogram trzeci

1. Miesiące: **czerwiec**, **lipiec**, **sierpień**.
2. Dni: **1**, **15**.
3. Raz o: **22:00:00**.
4. Obowiązuje:

   Od: **1 listopada 2009**.

   Do: **nie ustawiono**.

5.4 Po zdarzeniu zarejestrowanym w dzienniku systemu Windows

Ten typ harmonogramu ma zastosowanie tylko w systemach operacyjnych Windows.

Można zaplanować zadanie tworzenia kopii zapasowej po zarejestrowaniu danego zdarzenia w systemie Windows w jednym z dzienników zdarzeń, takim jak dziennik aplikacji, bezpieczeństwa lub systemowy.

Można na przykład skonfigurować plan tworzenia kopii zapasowych, który zapewni automatyczne wykonanie pełnej awaryjnej kopii zapasowej danych, kiedy tylko system Windows wykryje zbliżającą się awarię dysku twardego.

Parametry

Nazwa dziennika

Określa nazwę dziennika. Wybierz nazwę dziennika standardowego (**Aplikacja**, **Bezpieczeństwo** lub **System**) z listy lub wpisz nazwę dziennika — na przykład: **Microsoft Office Sessions**

Źródło zdarzenia

Określa źródło zdarzenia, zwykle wskazując komponent programu lub systemu, który spowodował zdarzenie — na przykład: **dysk**

Typ zdarzenia

Określa typ zdarzenia: **Błąd**, **Ostrzeżenie**, **Informacja**, **Powodzenie inspekcji** lub **Niepowodzenie inspekcji**.

Identyfikator zdarzenia

Określa numer zdarzenia, który zwykle umożliwia identyfikację konkretnego rodzaju zdarzeń wśród zdarzeń o takim samym źródle.

Na przykład zdarzenie **Błąd** o źródle **dysk** i identyfikatorze **7** występuje po wykryciu przez system Windows uszkodzonego sektora na dysku, natomiast zdarzenie **Błąd** o źródle **dysk** i identyfikatorze **15** występuje, kiedy dysk nie jest jeszcze gotowy do użycia.

Przykłady

Awaryjna kopia zapasowa po wykryciu „uszkodzonych sektorów”

Jeżeli na dysku twardym nagle pojawi się jeden lub więcej uszkodzonych sektorów, oznacza to, że wkrótce nastąpi awaria dysku twardego. Załóżmy, że chcesz utworzyć plan kopii zapasowych, który spowoduje skopiowanie danych z dysku twardego, gdy tylko wystąpi takie niebezpieczeństwo.

Kiedy system Windows wykryje uszkodzony sektor na dysku twardym, rejestruje zdarzenie o źródle **dysk** i identyfikatorze **7** w dzienniku **System**. Typ tego zdarzenia to **Błąd**.

Tworząc plan, wpisz lub wybierz następujące parametry w obszarze **Harmonogram**:

- **Nazwa dziennika**: **System**
- **Źródło zdarzenia**: **dysk**
- **Typ zdarzenia**: **Błąd**
- **Identyfikator zdarzenia**: **7**

Ważne: *Aby zapewnić wykonanie tego zadania pomimo obecności sektorów uszkodzonych, trzeba wybrać ignorowanie takich sektorów w tym zadaniu. Aby to zrobić w* ***Opcje tworzenia kopii zapasowej****, przejdź do* ***Obsługa błędów****, a następnie zaznacz pole wyboru* ***Ignoruj sektory uszkodzone****.*

Kopia zapasowa przed aktualizacją w systemie Vista

Załóżmy, że chcesz utworzyć plan tworzenia kopii zapasowych, który zapewni automatyczne wykonanie kopii zapasowej systemu — na przykład woluminu, na którym zainstalowany jest system Windows — przed instalacją każdej aktualizacji w systemie Windows.

Po pobraniu jednej lub więcej aktualizacji i zaplanowaniu ich instalacji, system operacyjny Microsoft Windows Vista rejestruje zdarzenie o źródle **Microsoft-Windows-WindowsUpdateClient** i identyfikatorze **18** w dzienniku **System**. Typ tego zdarzenia to **Informacja**.

Tworząc plan, wpisz lub wybierz następujące parametry w obszarze **Harmonogram**:

- **Nazwa dziennika**: **System**
- **Źródło zdarzenia**: **Microsoft-Windows-WindowsUpdateClient**
- **Typ zdarzenia**: **Informacja**
- **Identyfikator zdarzenia**: **18**

Wskazówka: *Aby skonfigurować podobny plan tworzenia kopii zapasowych dla komputerów z systemem Microsoft Windows XP, zastąp tekst w* ***Źródło zdarzenia*** *na* ***Agent aktualizacji Windows*** *i pozostaw niezmienione inne pola.*

Jak wyświetlić zdarzenia w Podglądzie zdarzeń

Otwieranie dziennika w Podglądzie zdarzeń

1. Na pulpicie lub w menu **Start** kliknij prawym przyciskiem myszy **Mój komputer**, a następnie **Zarządzaj**.
2. W konsoli **Zarządzanie komputerem**, rozwiń **Narzędzia systemowe**, a następnie **Podgląd zdarzeń**.
3. W pozycji **Podgląd zdarzeń** kliknij nazwę dziennika, który chcesz zobaczyć — na przykład **Aplikacja**.

   Uwaga: *Aby otworzyć dziennik bezpieczeństwa (****Bezpieczeństwo****), musisz być członkiem grupy administratorów.*

Wyświetlanie właściwości zdarzenia, w tym źródła i numeru zdarzenia

1. W pozycji **Podgląd zdarzeń** kliknij nazwę dziennika, który chcesz zobaczyć — na przykład **Aplikacja**.

   Uwaga: *Aby otworzyć dziennik bezpieczeństwa (****Bezpieczeństwo****), musisz być członkiem grupy administratorów.*

2. W liście zdarzeń w prawym panelu kliknij dwukrotnie nazwę zdarzenia, którego właściwości chcesz wyświetlić.
3. W oknie dialogowym **Właściwości zdarzenia** możesz wyświetlić właściwości zdarzenia, takie jak źródło zdarzenia pokazane w polu **Źródło** oraz numer zdarzenia pokazany w polu **Identyfikator zdarzenia**.

Po skończeniu kliknij **OK** , aby zamknąć okno dialogowe **Właściwości zdarzenia**.

5.5 Zaawansowane ustawienia harmonogramu

Po skonfigurowaniu w zasadach tworzenia kopii zapasowych harmonogramu dziennego, tygodniowego lub miesięcznego dostępne są poniższe ustawienia zaawansowane.

Użyj Wake-on-LAN

Po włączeniu tego ustawienia serwer Acronis Backup & Recovery 10 Management Server użyje funkcji Wake-on-LAN (WOL), aby o godzinie zaplanowanego utworzenia kopii zapasowej wznowić pracę wyłączonych komputerów zarejestrowanych. Jeśli zadania tworzenia kopii zapasowej na poszczególnych komputerach rozpoczynają się z opóźnieniem (zobacz następne ustawienie), serwer zarządzania wznowi pracę komputerów zgodnie z określonymi opóźnieniami.

Przed zastosowaniem tego ustawienia należy się upewnić, że funkcja Wake-on-LAN jest włączona na zarejestrowanych komputerach. Konfiguracje podstawowego systemu wyjścia/wejścia (BIOS), karty sieciowej i systemu operacyjnego muszą zezwalać na wznawianie pracy komputera ze stanu wyłączonego, nazywanego również stanem zasilania S5 lub G2.

Rozłóż uruchomienie w przedziale czasu

Po włączeniu tego ustawienia zadanie tworzenia kopii zapasowej na poszczególnych zarejestrowanych komputerach rozpocznie się z określonym opóźnieniem w stosunku do godziny rozpoczęcia ustawionej w zasadach. Dzięki temu następuje rozłożenie faktycznych godzin rozpoczęcia zadań w ramach pewnego przedziału czasowego.

Ustawienie to można zastosować podczas definiowania zasad tworzenia kopii zapasowych wielu komputerów w lokalizacji sieciowej, chcąc przez to uniknąć nadmiernego przeciążenia sieci.

Wartości opóźnienia wynoszą od zera do określonego maksimum i są ustalane na podstawie wybranej metody rozkładu.

Wartość opóźnienia dla poszczególnych komputerów jest ustalana podczas wdrażania zasad na tych komputerach. Pozostaje ona niezmienna do chwili ewentualnej edycji zasad i zmiany maksymalnej wartości opóźnienia.

Spełnienie ewentualnych warunków jest sprawdzane o faktycznej godzinie rozpoczęcia zadania na każdym z komputerów.

Poniższe przykłady przedstawiają zastosowanie tego ustawienia.

Przykład 1

Załóżmy, że na trzech komputerach są wdrażane zasady tworzenia kopii zapasowych według następującego harmonogramu:

Uruchom zadanie: **Codziennie**
Raz o: **09:00:00** .

Rozłóż uruchomienie w przedziale czasu
Maksymalne opóźnienie: **1 godzina**
Metoda rozkładu: **Losowa**

Wówczas na każdym z komputerów zadanie może rozpocząć się o dowolnej godzinie między 09:00:00 a 09:59:59 — na przykład:

Pierwszy komputer: codziennie o 09:30:03

Drugi komputer: codziennie o 09:00:00

Trzeci komputer: codziennie o 09:59:59

Przykład 2

Załóżmy, że na trzech komputerach są wdrażane zasady tworzenia kopii zapasowych według następującego harmonogramu:

Uruchom zadanie: **Codziennie**
Co: **2 godziny** Od: **09:00:00** Do: **11:00:00**

Rozłóż uruchomienie w przedziale czasu
Maksymalne opóźnienie: **1 godzina**
Metoda rozkładu: **Losowa**

Wówczas pierwsze uruchomienie zadania na każdym z komputerów może nastąpić o dowolnej godzinie między 09:00:00 a 09:59:59 . Przerwa między pierwszym a drugim uruchomieniem wynosi dokładnie dwie godziny — na przykład:

Pierwszy komputer: codziennie o 09:30:03 oraz 11:30:03

Drugi komputer: codziennie o 09:00:00 oraz 11:00:00

Trzeci komputer: codziennie o 09:59:59 oraz 11:59:59

Aby określić ustawienia zaawansowane

1. Połącz się z serwerem zarządzania lub z zarejestrowanym na nim komputerem, a następnie rozpocznij definiowanie zasad lub planu tworzenia kopii zapasowych.
2. W sekcji **Sposób tworzenia kopii zapasowej** wybierz Prosty, Wieża Hanoi lub Schemat niestandardowy, a następnie kliknij **Zmień**, aby określić harmonogram schematu.
3. W sekcji **Uruchom zadanie** wybierz **Codziennie**, **Co tydzień** lub **Co miesiąc**.
4. W obszarze **Ustawienia zaawansowane** kliknij **Zmień**.
5. Aby włączyć funkcję Wake-on-LAN, zaznacz pole wyboru **Użyj Wake-on-LAN**.
6. Aby rozłożyć godziny rozpoczęcia scentralizowanych zadań tworzenia kopii zapasowych, zaznacz pole wyboru **Rozłóż uruchomienie w przedziale czasu**, a następnie określ maksymalną wartość opóźnienia oraz metodę rozkładu.

5.6 W przypadku alertu programu Acronis Drive Monitor

Ten harmonogram ma zastosowanie w systemach operacyjnych Windows, w których jest zainstalowany program Acronis® Drive Monitor™.

Program Acronis Drive Monitor tworzy raporty na temat kondycji dysku twardego, korzystając z wewnętrznego systemu monitorowania tego dysku (S.M.A.R.T.). Na podstawie alertów programu Acronis Drive Monitor możesz skonfigurować awaryjne kopie zapasowe danych w uzupełnieniu regularnych kopii zapasowych. Tworzenie awaryjnej kopii zapasowej rozpoczyna się, gdy dyskowi zawierającemu dane grozi uszkodzenie.

Tworzenie kopii zapasowej rozpoczyna się natychmiast po osiągnięciu przez kondycję dysku poziomu ostrzegawczego lub krytycznego. Wskaźniki kondycji poszczególnych dysków (jako wartości procentowe) możesz sprawdzić, otwierając program Acronis Drive Monitor.

Alerty dotyczące temperatury dysku nie powodują rozpoczęcia tworzenia kopii zapasowej.

Wskazówka: *Jeśli plan tworzenia kopii zapasowych używa niestandardowego schematu tworzenia kopii zapasowych (s. 243), możesz skonfigurować tworzenie awaryjnej kopii zapasowej, dodając dodatkowy harmonogram do tego samego planu tworzenia kopii zapasowych. Jeśli jest używany inny schemat tworzenia kopii zapasowych, musisz utworzyć osobny plan tworzenia kopii zapasowych.*

5.7 Warunki

Warunki zwiększają elastyczność harmonogramu, ponieważ zadania tworzenia kopii zapasowych mogą być wykonywane zgodnie z podanymi warunkami. Gdy wystąpi określone zdarzenie (lista dostępnych zdarzeń znajduje się w sekcji „Tworzenie harmonogramu (s. 185)"), funkcja harmonogramu sprawdza określony warunek i w przypadku jego spełnienia wykonuje zadanie.

Gdy wystąpi zdarzenie, a warunek (lub jeden z wielu warunków) nie zostanie spełniony, działanie funkcji harmonogramu określa opcja tworzenia kopii zapasowych **Warunki uruchomienia zadania** (s. 129). Umożliwia ona określenie ważności warunków w strategii tworzenia kopii zapasowych:

- Spełnienie warunków jest obowiązkowe — zadanie tworzenia kopii zapasowej zostaje wstrzymane do czasu spełnienia wszystkich warunków.
- Spełnienie warunków jest preferowane, ale zadanie tworzenia kopii zapasowej ma wyższy priorytet — zadanie zostaje wstrzymane na pewien czas. Jeśli po upływie tego czasu warunki nadal pozostaną niespełnione, zadanie mimo to zostanie uruchomione. Przy tym ustawieniu program automatycznie rozwiązuje sytuację, w której warunki pozostają zbyt długo niespełnione, a dalsze opóźnianie kopii zapasowej jest niepożądane.
- Znaczenie ma czas uruchomienia zadania kopii zapasowej — zadanie tworzenia kopii zapasowej jest pomijane, jeżeli w chwili jego zaplanowanego uruchomienia warunki nie są spełnione. Pominięcie zadania jest sensowne, gdy kopię zapasową trzeba utworzyć o ściśle określonej godzinie, szczególnie w przypadku stosunkowo częstego występowania zdarzeń.

Warunki są dostępne tylko w przypadku korzystania z niestandardowego schematu tworzenia kopii zapasowych (s. 243). Warunki dla pełnych, przyrostowych i różnicowych kopii zapasowych można ustawić osobno.

Dodawanie wielu warunków

Aby umożliwić wykonanie zadania, wymagane jest jednoczesne spełnienie wielu warunków.

Przykład:

Zadanie tworzenia kopii zapasowej należy uruchomić, gdy na komputerze zarządzanym ilość wolnego miejsca zmieni się o przynajmniej 1 GB, ale tylko wtedy, gdy wszyscy użytkownicy są wylogowani i gdy od ostatniego utworzenia kopii zapasowej upłynęło ponad 12 godzin.

Harmonogram, warunki i opcję tworzenia kopii zapasowej **Warunki uruchomienia zadania** należy skonfigurować w następujący sposób:

- Harmonogram: **Gdy zmieni się ilość wolnego miejsca**; wartość: Uruchom zadanie, gdy ilość wolnego miejsca zmieni się o co najmniej: **1 GB**.
- Warunek: **Użytkownik wylogowany**; wartość: Uruchom zadanie zgodnie z planem tylko w przypadku, gdy wszyscy użytkownicy są wylogowani.
- Warunek: **Czas od utworzenia ostatniej kopii zapasowej**; wartość: Czas od utworzenia ostatniej kopii zapasowej: **12 godzin**.
- Warunki uruchomienia zadania: **Poczekaj na spełnienie warunków**.

Jeżeli ilość wolnego miejsca zmieni się o więcej niż 1 GB, funkcja harmonogramu poczeka na spełnienie obu pozostałych warunków i wówczas nastąpi uruchomienie zadania tworzenia kopii zapasowej.

5.7.1 Użytkownik jest bezczynny

Dotyczy: Windows

„Użytkownik jest bezczynny” oznacza, że na komputerze zarządzanym uruchomiony jest wygaszacz ekranu lub komputer jest zablokowany.

Przykład:

Uruchom zadanie tworzenia kopii zapasowych na komputerze zarządzanym codziennie o 21.00, najlepiej kiedy użytkownik jest bezczynny. Jeśli użytkownik będzie nadal aktywny do godziny 23.00, uruchom zadanie pomimo wszystko.

- Zdarzenie: **Codziennie**, co **1** dzień/dni; Raz o: **21:00:00**.
- Warunek: **Użytkownik jest bezczynny**.
- Warunki rozpoczęcia zadania: **Poczekaj na spełnienie warunków**. Uruchom zadanie po upływie **2** godzin(y).

Wskutek tego:

(1) Jeśli użytkownik przejdzie w stan bezczynności przed 21.00, zadanie tworzenia kopii zapasowej rozpocznie się o 21.00.

(2) Jeśli użytkownik przejdzie w stan bezczynności pomiędzy 21.00 a 23.00, zadanie tworzenia kopii zapasowej rozpocznie się natychmiast po wejściu w stan bezczynności.

(3) Jeśli jeden z użytkowników będzie nadal zalogowany o 23.00, tworzenie kopii zapasowej rozpocznie się pomimo wszystko.

5.7.2 Lokalizacja jest dostępna

Dotyczy: Windows, Linux

„Lokalizacja jest dostępna” oznacza, że docelowe miejsce przechowywania archiwów na dysku sieciowym jest dostępne w celu utworzenia kopii zapasowej.

Przykład:

Tworzenie kopii zapasowej w lokalizacji sieciowej odbywa się w dni robocze o 21.00. Jeśli lokalizacja o tej porze jest niedostępna (np. z powodu prac konserwacyjnych), pomiń tworzenie kopii zapasowej i poczekaj do następnego dnia roboczego, aby rozpocząć zadanie. Zakłada się, że zadanie raczej nie powinno wcale się rozpocząć niż zakończyć niepomyślnie.

- Zdarzenie: **Co tydzień**, Co **1** tydzień/tyg. w **<dni robocze>**; Raz o **21:00:00**.
- Warunek: **Lokalizacja jest dostępna**
- Warunki uruchomienia zadania: **Pomiń wykonywanie zadania**.

Wskutek tego:

(1) Jeśli nadejdzie 21.00 i lokalizacja archiwum będzie dostępna, zadanie tworzenia kopii zapasowej rozpocznie się dokładnie o tej godzinie.

(2) Jeśli nadejdzie 21.00, a lokalizacja archiwum będzie niedostępna, zadanie tworzenia kopii zapasowej rozpocznie się w następnym dniu roboczym, w którym lokalizacja będzie dostępna.

(3) Jeśli lokalizacja nie będzie dostępna w żaden dzień roboczy o godzinie 21.00, zadanie nie rozpocznie się nigdy.

5.7.3 Mieści się w przedziale czasu

Dotyczy: Windows, Linux

Ogranicza porę rozpoczęcia tworzenia kopii zapasowej do określonego interwału czasowego.

Przykład

Firma używa pamięci masowej w różnych lokalizacjach tej samej sieci w celu tworzenia kopii zapasowych danych użytkowników i serwerów. Dzień roboczy rozpoczyna się o 8.00 i kończy o 17.00. Kopia bezpieczeństwa danych użytkowników jest tworzona natychmiast po wylogowaniu użytkowników, ale nie wcześniej niż o 16.30 i nie później niż o 22.00. Kopia zapasowa danych na serwerze jest tworzona codziennie o 23.00. Zatem najlepiej utworzyć kopię zapasową danych wszystkich użytkowników przed tą godziną, aby nie blokować przepustowości sieci. Określając górny limit na 22.00, zakłada się, że tworzenie kopii zapasowych danych użytkowników nie zajmie więcej niż godzinę. Jeżeli jakiś użytkownik nadal będzie zalogowany w określonym interwale czasowym lub wyloguje się o dowolnej innej porze — kopia zapasowa danych użytkowników nie jest tworzona, to znaczy wykonanie zadania zostaje pominięte.

- Zdarzenie: **Przy wylogowywaniu**, Następujący użytkownik: **Dowolny użytkownik**.
- Warunek: **Mieści się w przedziale czasu**, od **16:30:00** do **22:00:00**.
- Warunki uruchomienia zadania: **Pomiń wykonywanie zadania**.

Wskutek tego:

(1) jeśli użytkownik wyloguje się pomiędzy 16:30:00 a 22:00:00, tworzenie kopii zapasowej rozpocznie się natychmiast po wylogowaniu;

(2) jeśli użytkownik wyloguje się o dowolnej innej porze, wykonanie zadania zostanie pominięte.

Co jeśli...

Co jeśli według harmonogramu zadanie ma być wykonane o określonej porze, a pora ta nie mieści się w określonym interwale czasu?

Na przykład:

- Zdarzenie: **Codziennie**, Co **1** dzień; Raz o **15:00:00** .
- Warunek: **Mieści się w przedziale czasu**, od **18:00:00** do **23:59:59** .

W tym przykładzie to, czy i kiedy zadanie zostanie uruchomione, zależy od warunków uruchomienia zadania:

- Jeśli warunek uruchomienia zadania to **Pomiń wykonywanie zadania**, zadanie nie zostanie uruchomione nigdy.
- Jeśli warunek uruchomienia zadania to **Poczekaj na spełnienie warunków**, a pole wyboru **Uruchom zadanie po upływie** będzie *odznaczone*, zadanie (zaplanowane na 15.00) rozpocznie się o 18.00 — o godzinie, kiedy warunek zostanie spełniony.
- Jeśli warunek uruchomienia zadania to **Poczekaj na spełnienie warunków**, a pole wyboru **Uruchom zadanie po upływie** będzie *zaznaczone* z czasem oczekiwania powiedzmy **1 godzina**, zadanie (zaplanowane na 15.00) rozpocznie się o 16.00 — o godzinie, kiedy skończy się okres oczekiwania.

5.7.4 Użytkownik wylogowany

Dotyczy: Windows

Uruchomienie zadania tworzenia kopii zapasowej zostaje wstrzymane do czasu, kiedy wszyscy użytkownicy wylogują się z systemu Windows na komputerze zarządzanym.

Przykład

Uruchom zadanie tworzenia kopii zapasowej o 20.00 w pierwszy i trzeci piątek każdego miesiąca, najlepiej po wylogowaniu wszystkich użytkowników. Jeśli o 23.00 jeden z użytkowników będzie nadal zalogowany, uruchom zadanie pomimo wszystko.

- Zdarzenie: **Co miesiąc**, Miesiące: **<Wszystkie>**; W: **<Pierwszy>**, **<Trzeci>** **<Piątek>**; Raz o **20:00:00**.
- Warunek: **Użytkownik wylogowany**.
- Warunki rozpoczęcia zadania: **Poczekaj na spełnienie warunków**. Uruchom zadanie po upływie **3** godzin.

Wskutek tego:

(1) jeśli wszyscy użytkownicy zostali wylogowani o 20.00, tworzenie kopii zapasowej rozpocznie się o 20.00;

(2) jeśli ostatni użytkownik wyloguje się pomiędzy 20.00 a 23.00, tworzenie kopii zapasowej rozpocznie się natychmiast po wylogowaniu;

(3) jeśli jeden z użytkowników będzie nadal zalogowany o 23.00, tworzenie kopii zapasowej rozpocznie się pomimo wszystko.

5.7.5 Czas od utworzenia ostatniej kopii zapasowej

Dotyczy systemu: Windows, Linux

Wykonywanie zadania tworzenia kopii zapasowej zostaje wstrzymane do momentu, aż od ostatniego pomyślnego utworzenia kopii zapasowej upłynie określony czas.

Przykład:

Zadanie tworzenia kopii zapasowej ma być uruchamiane przy uruchamianiu systemu, ale tylko wtedy, gdy od ostatniego pomyślnego utworzenia kopii zapasowej upłynęło ponad 12 godzin.

- Zdarzenie: **Przy uruchamianiu**; Rozpocznij zadanie po uruchomieniu komputera.
- Warunek: **Czas od utworzenia ostatniej kopii zapasowej**; Czas od utworzenia ostatniej kopii zapasowej: **12 godzin**.
- Warunki uruchomienia zadania: **Poczekaj na spełnienie warunków**.

Wskutek tego:

(1) Jeśli komputer zostanie ponownie uruchomiony przed upływem 12 godzin od ostatniego pomyślnego utworzenia kopii zapasowej, funkcja harmonogramu zaczeka, aż upłynie 12 godzin, i dopiero wtedy uruchomi zadanie.

(2) Jeśli komputer zostanie ponownie uruchomiony po upływie 12 godzin od ostatniego pomyślnego utworzenia kopii zapasowej, zadanie tworzenia kopii zapasowej rozpocznie się natychmiast.

(3) Jeśli komputer nie zostanie nigdy ponownie uruchomiony, zadanie nigdy się nie rozpocznie. W razie potrzeby tworzenie kopii zapasowej można uruchomić ręcznie w widoku **Plany i zadania tworzenia kopii zapasowych**.

6 Zarządzanie bezpośrednie

W tej sekcji opisano operacje, które można wykonywać bezpośrednio na komputerze zarządzanym przy użyciu bezpośredniego połączenia konsola-agent. Treść tej sekcji dotyczy zarówno autonomicznych, jak i zaawansowanych wersji programu Acronis Backup & Recovery 10.

6.1 Administrowanie komputerem zarządzanym

W tej sekcji opisano widoki dostępne za pośrednictwem drzewa nawigacji konsoli podłączonej do komputera zarządzanego oraz wyjaśniono sposób pracy z każdym widokiem.

6.1.1 Pulpit nawigacyjny

Pulpit nawigacyjny służy do szybkiego szacowania, czy dane są skutecznie chronione na komputerze. Pulpit nawigacyjny pokazuje podsumowanie działań agenta programu Acronis Backup & Recovery 10 oraz umożliwia błyskawiczne identyfikowanie i rozwiązywanie dowolnych problemów.

Alerty

Sekcja alertów zwraca uwagę użytkownika na problemy, które wystąpiły na komputerze, a także oferuje sposoby ich naprawiania i sprawdzania. Najpoważniejsze problemy są wyświetlane u góry. Jeśli w danej chwili nie ma żadnych alertów ani ostrzeżeń, system wyświetla komunikat „No alerts or warnings” (Brak alertów i ostrzeżeń).

Typy alertów

W poniższej tabeli przedstawiono typy możliwych komunikatów.

	Opis	Proponowane działanie	Komentarz
	Zadania zakończone niepowodzeniem: X	Rozpoznaj	Wybranie działania **Rozpoznaj** spowoduje otwarcie widoku **Plany i zadania tworzenia kopii zapasowych** z zadaniami zakończonymi niepowodzeniem, w którym można sprawdzić przyczynę niepowodzenia.
	Zadania wymagające działania: X	Rozpoznaj	Za każdym razem, gdy zadanie wymaga działania użytkownika, na pulpicie nawigacyjnym wyświetlany jest komunikat informujący o tym, jaką czynność należy wykonać (na przykład włożyć nową płytę CD lub zatrzymać/ponowić/zignorować w przypadku błędu).
	Nie można sprawdzić licencji bieżącej wersji. X dni zostało do zaprzestania pracy przez oprogramowanie. Upewnij się, że masz ważną licencję na serwerze licencji Acronis.	Połącz	Agent programu Acronis Backup & Recovery 10 łączy się z serwerem Acronis License Server po uruchomieniu, a następnie co 1–5 dni (domyślnie co 1 dzień), zgodnie z ustawieniami określonymi w parametrach konfiguracji agenta. Jeśli sprawdzenie licencji nie powiedzie się przez 1–60 dni (zgodnie z ustawieniem określonym w parametrach konfiguracji agenta — domyślnie 30 dni), agent przestanie działać do momentu

			pomyślnego sprawdzenia licencji.
	Nie można sprawdzić klucza licencji bieżącej wersji od X dni. Serwer licencji Acronis był niedostępny lub dane klucza licencji są uszkodzone. Sprawdź łączność z serwerem i uruchom serwer licencji Acronis, aby zarządzać licencjami. Upewnij się, że masz ważną licencję na serwerze licencji Acronis.	Połącz	Działanie programu Acronis Backup & Recovery 10 zostało zatrzymane. Przez ostatnie *X* dni agent nie mógł sprawdzić, czy na serwerze Acronis License Server jest dostępna jego licencja. Prawdopodobnie jest to spowodowane niedostępnością serwera licencji. Może być także konieczne sprawdzenie, czy na serwerze licencji znajdują się licencje lub czy dane klucza licencyjnego nie zostały uszkodzone. Po pomyślnym sprawdzeniu licencji agent rozpocznie działanie.
	Wersja próbna programu wygasa za *X* dni Upewnij się, że masz ważną licencję na serwerze licencji Acronis.	Połącz	Po zainstalowaniu wersji próbnej program rozpoczyna odliczanie dni pozostałych do końca okresu próbnego.
	Okres próbny zakończył się. Uruchom instalator i wprowadź klucz pełnej licencji. Upewnij się, że masz ważną licencję na serwerze licencji Acronis.	Połącz	Upłynął 15-dniowy okres próbny. Wprowadź pełny klucz licencyjny.
	Skarbce z małą ilością wolnego miejsca: X	Wyświetl skarbce	Wybranie działania **Wyświetl skarbce** spowoduje otwarcie widoku **Skarbce**, w którym można sprawdzić rozmiar, wolne miejsce i zawartość skarbca oraz wykonać czynności niezbędne do zwiększenia ilości wolnego miejsca.
	Nie utworzono nośnika startowego	Utwórz teraz	Aby mieć możliwość odzyskania systemu operacyjnego po niepomyślnym uruchomieniu komputera, należy: 1. Utworzyć kopię zapasową woluminu systemowego (i woluminu startowego, jeśli jest inny). 2. Utworzyć co najmniej jeden nośnik startowy (s. 424). Wybranie działania **Utwórz teraz** spowoduje uruchomienie Generatora nośnika startowego (s. 422).
	Nie utworzono kopii zapasowych od *X* dni	Utwórz kopię zapasową	Pulpit nawigacyjny ostrzega, że w ciągu stosunkowo długiego czasu na komputerze nie utworzono kopii zapasowej żadnych danych. Wybranie działania **Utwórz kopię zapasową** spowoduje wyświetlenie strony **Utwórz plan tworzenia kopii zapasowych**, na której można natychmiast skonfigurować i uruchomić operację tworzenia kopii zapasowej. Aby skonfigurować czas uważany za krytyczny, wybierz **Opcje > Opcje konsoli > Alerty związane z czasem**.

⚠	Brak połączenia z serwerem zarządzania od X dni	Wyświetl komputery	Tego rodzaju komunikat może być wyświetlany na komputerze zarejestrowanym na serwerze zarządzania. Pulpit nawigacyjny ostrzega o możliwości utraty połączenia lub niedostępności serwera, w wyniku czego komputer nie jest centralnie zarządzany.

Działania

Kalendarz umożliwia badanie historii działań agenta programu Acronis Backup & Recovery 10 na komputerze. Aby wyświetlić listę wpisów dziennika odfiltrowanych według daty, kliknij prawym przyciskiem myszy dowolną wyróżnioną datę, a następnie wybierz **Wyświetl dziennik**.

W sekcji **Widok** (po prawej stronie kalendarza) można wybrać działania, które będą wyróżniane w zależności od obecności i wagi błędów.

	Sposób ustalania
Błędy	Data jest wyróżniona kolorem czerwonym, jeśli w dzienniku przy tej dacie pojawia się co najmniej jeden wpis „Błąd”.
Ostrzeżenia	Data jest wyróżniona kolorem żółtym, jeśli w dzienniku przy tej dacie nie pojawia się żaden wpis „Błąd”, natomiast pojawia się co najmniej jeden wpis „Ostrzeżenie”.
Informacja	Data jest wyróżniona kolorem zielonym, jeśli przy tej dacie pojawiają się wyłącznie wpisy dziennika „Informacja” (normalne działanie).

Łącze **Select current date** (Wybierz bieżącą datę) koncentruje wybór na bieżącej dacie.

Widok systemu

Przedstawia podsumowanie statystyk dotyczących planów i zadań tworzenia kopii zapasowych oraz krótkie informacje o ostatniej kopii zapasowej. Aby uzyskać odpowiednie informacje, należy kliknąć elementy w tej sekcji. Spowoduje to wyświetlenie widoku **Plany i zadania tworzenia kopii zapasowych** (s. 205) zawierającego wstępnie odfiltrowane plany lub zadania. Na przykład kliknięcie elementu **Lokalne** w sekcji **Plany tworzenia kopii zapasowych** spowoduje otwarcie widoku **Plany i zadania tworzenia kopii zapasowych** zawierającego plany tworzenia kopii zapasowych odfiltrowane według źródła **Lokalne**.

Zadania wymagające działania

W tym oknie znajdują się wszystkie zadania wymagające działania użytkownika. Umożliwia ono podjęcie decyzji, na przykład o potwierdzeniu ponownego uruchomienia lub ponowieniu próby po zwolnieniu miejsca na dysku, dotyczącej każdego z zadań. Dopóki co najmniej jedno zadanie wymaga działania, to okno można otworzyć w dowolnym momencie za pomocą **pulpitu nawigacyjnego** (s. 202) komputera zarządzanego.

Zaznaczenie pola wyboru parametru **Nie wyświetlaj tego okna, gdy zadania wymagają działania. Informacje będą dostępne w oknie szczegółowych informacji o zadaniu i na pulpicie nawigacyjnym.** spowoduje wyświetlenie zadań na **pulpicie nawigacyjnym** razem z innymi alertami i ostrzeżeniami.

Można również przejrzeć stany wykonania zadań w widoku **Plany i zadania tworzenia kopii zapasowych** (s. 205) oraz podjąć decyzję dotyczącą każdego zadania w panelu **Informacja** (lub w oknie **Szczegóły zadania** (s. 213)).

6.1.2 Plany i zadania tworzenia kopii zapasowych

Widok **Plany i zadania tworzenia kopii zapasowych** zawiera informacje o ochronie danych na określonym komputerze. Pozwala monitorować plany i zadania tworzenia kopii zapasowych oraz zarządzać nimi.

Plan tworzenia kopii zapasowych to zestaw reguł, które określają, w jaki sposób konkretne dane będą chronione na określonym komputerze. Fizycznie plan tworzenia kopii zapasowych to komplet zadań skonfigurowanych do wykonywania na komputerze zarządzanym. Aby dowiedzieć się, jakie zadania w danym momencie wykonuje plan tworzenia kopii zapasowych, należy sprawdzić stan wykonania planu tworzenia kopii zapasowych (s. 205). Stan planu tworzenia kopii zapasowych to skumulowany stan zadań planu. Status planu tworzenia kopii zapasowych (s. 206) ułatwia szacowanie, czy dane są skutecznie chronione.

Zadanie to zestaw kolejnych czynności, które będą wykonywane na komputerze po nadejściu określonej godziny lub po wystąpieniu określonego zdarzenia. W celu śledzenia bieżącego postępu zadania należy sprawdzić jego stan (s. 207). Sprawdzając status (s. 208) zadania, można ustalić jego wynik.

Sposób pracy

- Aby wyświetlić żądane plany (zadania) tworzenia kopii zapasowych w tabeli planów tworzenia kopii zapasowych, należy użyć filtrów. Domyślnie w tabeli są wyświetlane wszystkie plany komputera zarządzanego posortowane według nazwy. Można również ukrywać niepotrzebne kolumny i wyświetlać ukryte. Aby uzyskać szczegółowe informacje, zobacz Filtrowanie oraz sortowanie planów i zadań tworzenia kopii zapasowych (s. 212).
- W tabeli kopii zapasowych należy wybrać plan (zadanie) tworzenia kopii zapasowych.
- Aby wykonać czynność dotyczącą wybranego planu (zadania), należy użyć przycisków paska narzędzi. Aby uzyskać szczegółowe informacje, zobacz sekcję Czynności dotyczące planów tworzenia kopii zapasowych i zadań (s. 209). Utworzone plany i zadania można uruchamiać, edytować, zatrzymywać i usuwać.
- Panel **Informacja** służy do przeglądania szczegółowych informacji na temat wybranego planu (zadania). Panel jest domyślnie zwinięty. Aby rozwinąć panel, należy kliknąć przycisk. Zawartość panelu jest także zduplikowana odpowiednio w oknach **Szczegóły planu** (s. 215) i **Szczegóły zadania** (s. 213).

Opis stanów i statusów

Stany wykonania planu tworzenia kopii zapasowej

Plan tworzenia kopii zapasowych może mieć jeden z następujących stanów wykonania: **Bezczynne, Oczekujące, Uruchomione, Zatrzymywane, Wymagające działania**.

Nazwy stanów planu są takie same jak nazwy stanów zadań, ponieważ stan planu to łączny stan jego poszczególnych zadań.

	Stan	Sposób ustalania	Sposób postępowania
1	**Wymagające działania**	Co najmniej jedno zadanie wymaga działania użytkownika. W przeciwnym razie zobacz 2.	Zidentyfikuj zadania wymagające działania (program wyświetli informacje o wymaganej czynności) -> Zatrzymaj zadania lub stwórz warunki do ich wykonywania (zmień nośnik, udostępnij dodatkowe miejsce w skarbcu, zignoruj błąd odczytu, utwórz brakującą strefę Acronis Secure Zone).

2	**Uruchomione**	Co najmniej jedno zadanie jest uruchomione. W przeciwnym razie zobacz 3.	Nie trzeba wykonywać żadnej czynności.
3	**Oczekujące**	Co najmniej jedno zadanie oczekuje. W przeciwnym razie zobacz 4.	Oczekiwanie na spełnienie warunku. Ta sytuacja jest zupełnie normalna, ale zbyt długie opóźnianie tworzenia kopii zapasowej jest ryzykowne. Rozwiązaniem może być ustawienie maksymalnego opóźnienia lub wymuszenie spełnienia warunku (poinformowanie użytkownika o konieczności wylogowania, włączenie wymaganego połączenia sieciowego). Oczekiwanie na odblokowanie niezbędnych zasobów przez inne zadanie. W odosobnionych przypadkach oczekiwanie może być konieczne, gdy z jakiegoś powodu uruchomienie zadania opóźnia się lub jego wykonywanie trwa dużo dłużej niż zwykle, co nie pozwala uruchomić innego zadania. Tego rodzaju problem znika automatycznie po zakończeniu zadania stanowiącego przeszkodę. Jeśli wykonywanie zadania trwa zbyt długo, czasem warto je zatrzymać, aby umożliwić uruchomienie następnego zadania. Trwałe nakładanie się zadań może wynikać z planu lub planów o niepoprawnym harmonogramie. W takim przypadku warto zmodyfikować plan.
4	**Zatrzymywane**	Co najmniej jedno zadanie jest zatrzymywane. W przeciwnym razie zobacz 5.	Nie trzeba wykonywać żadnej czynności.
5	**Bezczynne**	Wszystkie zadania są bezczynne.	Nie trzeba wykonywać żadnej czynności.

Statusy planu tworzenia kopii zapasowych

Plan tworzenia kopii zapasowych może mieć jeden z następujących statusów: **Błąd, Ostrzeżenie, OK**.

Status planu tworzenia kopii zapasowych pochodzi z wyników ostatniego uruchomienia zadań planu.

	Status	Sposób ustalania	Sposób postępowania
1	**Błąd**	Co najmniej jedno zadanie zakończyło się niepowodzeniem. W przeciwnym razie zobacz 2.	Zidentyfikuj zadania zakończone niepowodzeniem -> Sprawdź dziennik zadań, aby poznać przyczynę niepowodzenia, a następnie wykonaj co najmniej jedną z poniższych czynności: ▪ Usuń przyczynę niepowodzenia -> [opcjonalnie] Ręcznie uruchom zadanie zakończone niepowodzeniem. ▪ Jeśli niepowodzeniem zakończył się plan lokalny, zmodyfikuj go, aby zapobiec niepowodzeniu w przyszłości. ▪ Jeśli niepowodzeniem zakończył się plan scentralizowany, zmodyfikuj zasady tworzenia kopii zapasowych na serwerze zarządzania. Podczas definiowania planu lub zasad tworzenia kopii zapasowych administrator może włączyć opcję, która powoduje zatrzymanie wykonywania planu z chwilą wystąpienia w nim

			statusu Błąd. Wykonywanie planu tworzenia kopii zapasowych można wznowić przyciskiem Uruchom ponownie.
2	**Ostrzeżenie**	Co najmniej jedno zadanie zakończyło się pomyślnie z ostrzeżeniami. W przeciwnym razie zobacz 3.	Wyświetl dziennik, aby przeczytać ostrzeżenia -> [opcjonalnie] Wykonaj odpowiednie czynności, aby zapobiec ostrzeżeniom lub niepowodzeniu w przyszłości.
3	**OK**	Wszystkie zadania zakończyły się pomyślnie.	Nie trzeba wykonywać żadnej czynności. Należy pamiętać, że plan tworzenia kopii zapasowych może mieć status OK w przypadku, gdy nie uruchomiono jeszcze żadnych zadań bądź gdy niektóre zadania zostały zatrzymane lub są zatrzymywane. Te sytuacje uważa się za normalne.

Stany zadania

Zadanie może mieć jeden z następujących stanów: **Bezczynne**, **Oczekujące**, **Uruchomione**, **Zatrzymywane**, **Wymagające działania**. Początkowym stanem zadania jest **Bezczynne**.

Po ręcznym uruchomieniu zadania lub wystąpieniu zdarzenia określonego przez harmonogram zadanie przechodzi w stan **Uruchomione** lub **Oczekujące**.

Uruchomione

Stan zadania zmienia się na **Uruchomione**, gdy wystąpiło zdarzenie określone przez harmonogram, zostały spełnione wszystkie warunki ustawione w planie tworzenia kopii zapasowych ORAZ nie jest uruchomione żadne inne zadanie, które blokuje potrzebne zasoby. W takim przypadku nic nie stoi na przeszkodzie, aby uruchomić zadanie.

Oczekujące

Stan zadania zmienia się na **Oczekujące**, gdy zadanie ma zostać uruchomione, ale jest już uruchomione inne zadanie, które używa tych samych zasobów. W szczególności nie można uruchomić na komputerze jednocześnie kilku zadań tworzenia kopii zapasowych lub odzyskiwania. Nie można również uruchomić jednocześnie zadania tworzenia kopii zapasowych i zadania odzyskiwania. Gdy inne zadanie odblokuje zasób, zadanie oczekujące przejdzie w stan **Uruchomione**.

Stan zadania może także zmienić się na **Oczekujące**, gdy wystąpiło zdarzenie określone przez harmonogram, ale nie został spełniony warunek ustawiony w planie tworzenia kopii zapasowych. Aby uzyskać szczegółowe informacje, zobacz Warunki uruchomienia zadania (s. 129).

Wymagające działania

Dowolne uruchomione zadanie może przejść w stan **Wymagające działania**, gdy jest konieczne działania człowieka, np. zmiana nośnika lub zignorowanie błędu odczytu. Następnym stanem może być **Zatrzymywane** (jeśli użytkownik wybierze zatrzymanie zadania) lub **Uruchomione** (w przypadku wybrania opcji zignorowania/ponowienia lub innej czynności, takiej jak ponowne uruchomienie, która spowoduje przejście zadania w stan **Uruchomione**).

Zatrzymywane

Użytkownik może zatrzymać uruchomione zadanie lub zadanie wymagające działania. Stan zadania zmieni się na **Zatrzymywane**, a następnie na **Bezczynne**. Zadanie oczekujące również można zatrzymać. Ponieważ zadanie nie jest uruchomione, w takim przypadku „zatrzymanie” oznacza usunięcie go z kolejki.

Diagram stanów zadania

Statusy zadania

Zadanie może mieć jeden z następujących statusów: **Błąd**, **Ostrzeżenie**, **OK**.

Status zadania pochodzi z wyniku ostatniego uruchomienia zadania.

	Status	Sposób ustalania	Sposób obsługi
1	**Błąd**	Ostatnim wynikiem jest „Niepowodzenie”.	Zidentyfikuj zadanie zakończone niepowodzeniem -> Sprawdź dziennik zadań, aby poznać przyczynę niepowodzenia, a następnie wykonaj co najmniej jedną z poniższych czynności: ▪ Usuń przyczynę niepowodzenia -> [opcjonalnie] Ręcznie uruchom zadanie zakończone niepowodzeniem. ▪ Przeprowadź edycję zadania zakończonego niepowodzeniem, aby zapobiec niepowodzeniu w przyszłości. ▪ Jeśli niepowodzeniem zakończył się plan lokalny, przeprowadź jego edycję, aby zapobiec niepowodzeniu w przyszłości. ▪ Jeśli niepowodzeniem zakończył się plan centralny, przeprowadź edycję zasad tworzenia kopii zapasowych na serwerze zarządzania.
2	**Ostrzeżenie**	Ostatnim wynikiem jest	Wyświetl dziennik, aby przeczytać ostrzeżenia ->

		„Wykonane pomyślnie z ostrzeżeniami”.	[opcjonalnie] Wykonaj odpowiednie czynności, aby zapobiec ostrzeżeniom lub niepowodzeniu w przyszłości.
3	**OK**	Ostatnim wynikiem jest „Wykonane pomyślnie”, „-” lub „Zatrzymane”.	Nie trzeba wykonywać żadnej czynności. Stan „-” oznacza, że zadanie nigdy nie zostało uruchomione bądź zostało uruchomione, ale jeszcze się nie zakończyło, więc jego wynik jest niedostępny.

Praca z planami i zadaniami tworzenia kopii zapasowych

Czynności dotyczące planów i zadań tworzenia kopii zapasowych

Poniżej przedstawiono wskazówki dotyczące wykonywania operacji na planach i zadaniach tworzenia kopii zapasowych.

Zadanie	Czynności
Utworzenie nowego planu lub zadania tworzenia kopii zapasowych	Kliknij **Nowy** i wybierz jedną z następujących opcji: ▪ Plan tworzenia kopii zapasowych (s. 219) ▪ Zadanie odzyskiwania ▪ Zadanie sprawdzania poprawności (s. 271)
Wyświetlanie szczegółów planu lub zadania	**Plan tworzenia kopii zapasowych** Kliknij **Wyświetl szczegóły**. W oknie **Szczegóły planu** (s. 215) przejrzyj szczegółowe informacje dotyczące planu. **Zadanie** Kliknij **Wyświetl szczegóły**. W oknie **Szczegóły zadania** (s. 213) przejrzyj szczegółowe informacje dotyczące zadania.
Wyświetlanie dziennika planu lub zadania	**Plan tworzenia kopii zapasowych** Kliknij **Wyświetl dziennik**. Nastąpi przejście do widoku **Dziennik** (s. 216), zawierającego listę wpisów dziennika dotyczących planu. **Zadanie** Kliknij **Wyświetl dziennik**. Nastąpi przejście do widoku **Dziennik** (s. 216), zawierającego listę wpisów dziennika dotyczących zadania.

Uruchamianie planu lub zadania	**Plan tworzenia kopii zapasowych** Kliknij **Uruchom**. W oknie **Uruchom plan tworzenia kopii zapasowych** (s. 213) wybierz zadanie, które chcesz uruchomić. Uruchomienie planu tworzenia kopii zapasowych powoduje natychmiastowe uruchomienie wybranego zadania, niezależnie od jego harmonogramu i warunków. *Dlaczego nie mogę uruchomić planu tworzenia kopii zapasowych?* ▪ Brak odpowiednich uprawnień. Jeśli użytkownik nie ma na komputerze uprawnień administratora, nie może uruchamiać planów należących do innych użytkowników. **Zadanie** Kliknij **Uruchom**. Zadanie zostanie wykonane natychmiast, niezależnie od harmonogramu i warunków.
Zatrzymywanie planu lub zadania	**Plan tworzenia kopii zapasowych** Kliknij **Zatrzymaj**. Zatrzymanie wykonywanego planu tworzenia kopii zapasowej powoduje zatrzymanie wszystkich jego zadań. Dlatego wszystkie operacje zadań zostaną przerwane. **Zadanie** Kliknij **Zatrzymaj**. *Co się stanie, jeśli zatrzymam zadanie?* Ogólnie rzecz biorąc, zatrzymanie zadania spowoduje przerwanie jego operacji (tworzenia kopii zapasowej, odzyskiwania, sprawdzania poprawności, eksportowania, konwersji, migracji). Zadanie przejdzie najpierw w stan Zatrzymywane, a następnie w stan Bezczynne. Ewentualny harmonogram zadania pozostanie ważny. Aby dokończyć operację, trzeba będzie uruchomić zadanie od początku. ▪ Zadanie odzyskiwania (z kopii zapasowej dysku): wolumin docelowy zostanie usunięty, a jego miejsce stanie się nieprzydzielone — tak samo jak w przypadku niepowodzenia odzyskiwania. Aby odzyskać „utracony” wolumin, należy ponownie uruchomić zadanie. ▪ Zadanie odzyskiwania (z kopii zapasowej plików): przerwana operacja może spowodować zmiany w folderze docelowym. W zależności od tego, w jakim momencie zadanie zostało zatrzymane, niektóre pliki mogą zostać odzyskane, a inne nie. Aby odzyskać wszystkie pliki, należy ponownie uruchomić zadanie.

Edytowanie planu lub zadania	**<u>Plan tworzenia kopii zapasowych</u>** Kliknij **Edytuj**. Edycja planu tworzenia kopii zapasowych odbywa się w ten sam sposób co jego tworzenie (s. 219), z wyjątkiem następujących **ograniczeń**: Jeśli utworzone archiwum nie jest puste (czyli zawiera kopie zapasowe), podczas edycji planu tworzenia kopii zapasowych nie zawsze można używać wszystkich opcji schematów. 1. Nie można zmienić schematu na Dziadek-ojciec-syn ani Wieża Hanoi. 2. Jeśli stosowany jest schemat Wieża Hanoi, nie jest możliwa zmiana liczby poziomów. We wszystkich innych przypadkach schemat można zmienić i powinien on nadal działać tak, jakby istniejące archiwa zostały utworzone na podstawie nowego schematu. W przypadku pustych archiwów możliwe są wszystkie zmiany. *Dlaczego nie mogę edytować planu tworzenia kopii zapasowych?* ▪ Plan tworzenia kopii zapasowych jest obecnie uruchomiony. Edycja uruchomionego planu tworzenia kopii zapasowych jest niemożliwa. ▪ Brak odpowiednich uprawnień. Jeśli użytkownik nie ma na komputerze uprawnień administratora, nie może edytować planów należących do innych użytkowników. ▪ Plan tworzenia kopii zapasowych ma pochodzenie centralne. Bezpośrednia edycja scentralizowanych planów tworzenia kopii zapasowych jest niemożliwa. Należy zmodyfikować oryginalne zasady tworzenia kopii zapasowych. **<u>Zadanie</u>** Kliknij **Edytuj**. *Dlaczego nie mogę edytować zadania?* ▪ Zadanie należy do planu tworzenia kopii zapasowych. Bezpośrednia edycja jest możliwa tylko w przypadku zadań, które nie należą do planu tworzenia kopii zapasowych, takich jak zadanie odzyskiwania. Jeśli zmian wymaga zadanie należące do lokalnego planu tworzenia kopii zapasowych, należy zmodyfikować ten plan. Zadanie należące do scentralizowanego planu tworzenia kopii zapasowych można zmodyfikować przez edycję scentralizowanych zasad będących źródłem tego planu. Może to zrobić tylko administrator serwera zarządzania. ▪ Brak odpowiednich uprawnień. Jeśli użytkownik nie ma na komputerze uprawnień administratora, nie może modyfikować zadań należących do innych użytkowników.

Usuwanie planu lub zadania	**Plan tworzenia kopii zapasowych** Kliknij **Usuń**. *Co się stanie, jeśli usunę plan tworzenia kopii zapasowych?* Usunięcie planu spowoduje usunięcie wszystkich jego zadań. *Dlaczego nie mogę usunąć planu tworzenia kopii zapasowych?* ▪ Plan tworzenia kopii zapasowych jest w stanie uruchomienia. Nie można usunąć planu tworzenia kopii zapasowych, jeśli uruchomione jest przynajmniej jedno z jego zadań. ▪ Brak odpowiednich uprawnień. Jeśli użytkownik nie ma na komputerze uprawnień administratora, nie może usuwać planów należących do innych użytkowników. ▪ Plan tworzenia kopii zapasowych ma pochodzenie centralne. Administrator serwera zarządzania może usunąć plan scentralizowany przez odwołanie zasad tworzenia kopii zapasowych, które spowodowały powstanie planu. **Zadanie** Kliknij **Usuń**. *Dlaczego nie mogę usunąć zadania?* ▪ Zadanie należy do planu tworzenia kopii zapasowych. Zadania należącego do planu tworzenia kopii zapasowych nie można usunąć w oderwaniu od planu. Zmodyfikuj plan tak, aby usunąć z niego zadanie, lub usuń cały plan. ▪ Brak odpowiednich uprawnień. Jeśli użytkownik nie ma na komputerze uprawnień administratora, nie może usuwać zadań należących do innych użytkowników.
Odświeżanie tabeli	Kliknij **Odśwież**. Konsola zarządzania zaktualizuje listę planów i zadań istniejących na komputerze z uwzględnieniem najnowszych informacji. Mimo że lista jest odświeżana automatycznie na podstawie zdarzeń, ze względu na pewne opóźnienie dane z komputera zarządzanego mogą nie pojawić się natychmiast. Po ręcznym odświeżeniu wyświetlane są najbardziej aktualne dane.

Filtrowanie oraz sortowanie planów i zadań tworzenia kopii zapasowych

Zadanie	Działanie
Sortuj plany i zadania tworzenia kopii zapasowych według: nazwy, stanu, statusu, typu, pochodzenia itp.	Kliknij nagłówek kolumny, aby posortować plany i zadania tworzenia kopii zapasowych w porządku rosnącym. Kliknij ponownie nagłówek kolumny, aby posortować plany i zadania w porządku malejącym.
Filtru plany/zadania według nazwy lub właściciela	Wpisz nazwę planu/zadania lub właściciela w polu pod odpowiednim nagłówkiem. Zostanie wyświetlona lista zadań, których nazwy/nazwy właścicieli są całkowicie lub częściowo zgodne z

	wprowadzoną wartością.
Filtruj plany i zadania według stanu, statusu, typu, pochodzenia, ostatniego wyniku lub harmonogramu	W polu pod odpowiednim nagłówkiem wybierz żądaną wartość z listy.

Konfigurowanie tabeli planów i zadań tworzenia kopii zapasowych

Domyślnie w tabeli jest wyświetlanych sześć kolumn, a pozostałe są ukryte. W razie potrzeby można ukryć wyświetlane kolumny i wyświetlić kolumny ukryte.

Aby wyświetlić lub ukryć kolumny

1. Kliknij prawym przyciskiem myszy nagłówek kolumny, aby wyświetlić menu kontekstowe. Zaznaczone elementy menu odpowiadają nagłówkom kolumn wyświetlanych w tabeli.
2. Kliknij elementy, które chcesz wyświetlić/ukryć.

Uruchom plan tworzenia kopii zapasowej

Plan tworzenia kopii zapasowych uważa się za uruchomiony, jeśli co najmniej jedno z jego zadań jest uruchomione. W oknie **Uruchom plan tworzenia kopii zapasowej** można uruchomić zadanie z wybranego planu tworzenia kopii zapasowych ręcznie, niezależnie od jego harmonogramu.

Aby uruchomić zadanie z wybranego planu tworzenia kopii zapasowych

1. Wybierz z planu tworzenia kopii zapasowych zadanie, które trzeba uruchomić. Aby upewnić się, że dokonany wybór jest prawidłowy, sprawdź informacje o zadaniu zgromadzone na kartach w dolnej części okna. Informacje te są także zduplikowane w oknie **Szczegóły zadania** (s. 213).
2. Kliknij **OK**.

Tymczasowe wyłączanie planu tworzenia kopii zapasowej

Tymczasowe wyłączenie planu tworzenia kopii zapasowych jest potrzebne podczas przenoszenia archiwów z jednego skarbca do innego za pomocą menedżera plików innej firmy.

Dotyczy to wyłącznie planów tworzenia kopii zapasowych, które używają niestandardowych schematów tworzenia kopii zapasowych.

Aby wyłączyć plan tworzenia kopii zapasowych

1. Kliknij **Edytuj**.
2. Wprowadź opcję planowania schematu tworzenia kopii zapasowych i wyłącz harmonogram dotyczący żądanego okresu, zmieniając parametry **Data rozpoczęcia** i/lub **End date** (Data zakończenia).

Szczegóły zadania

Okno **Task details** (Szczegóły zadania) (zduplikowane także na panelu **Informacje**) gromadzi wszystkie informacje dotyczące wybranego zadania.

Kiedy zadanie wymaga działania użytkownika, powyżej kart pojawiają się przyciski czynności i komunikat. Komunikat zawiera krótki opis problemu. Przyciski umożliwiają ponowienie lub zatrzymanie zadania albo planu tworzenia kopii zapasowych.

Typy zadań

W poniższej tabeli zestawiono wszystkie typy zadań dostępnych w programie Acronis Backup & Recovery 10. Rzeczywiste typy zadań dostępne dla użytkownika zależą od wersji programu i komponentu, do którego jest podłączona konsola.

Nazwa zadania	Opis
Kopia zapasowa (dysk)	Tworzenie kopii zapasowych dysków i woluminów
Kopia zapasowa (plik)	Tworzenie kopii zapasowych plików i folderów
Kopia zapasowa (maszyna wirtualna)	Tworzenie kopii zapasowej całej maszyny wirtualnej lub jej woluminów
Odzyskiwanie (dysk)	Odzyskiwanie kopii zapasowej dysku
Odzyskiwanie (plik)	Odzyskiwanie plików i folderów
Odzyskiwanie (wolumin)	Odzyskiwanie woluminów z kopii zapasowej dysku
Odzyskiwanie (główny rekord rozruchowy)	Odzyskiwanie głównego rekordu rozruchowego
Odzyskiwanie (dysk, na istniejącej maszynie wirtualnej)	Odzyskiwanie kopii zapasowej dysku/woluminu na istniejącej maszynie wirtualnej
Odzyskiwanie (dysk, na nowej maszynie wirtualnej)	Odzyskiwanie kopii zapasowej dysku/woluminu na nowej maszynie wirtualnej
Odzyskiwanie (istniejąca maszyna wirtualna)	Odzyskiwanie kopii zapasowej maszyny wirtualnej na istniejącej maszynie wirtualnej
Odzyskiwanie (nowa maszyna wirtualna)	Odzyskiwanie kopii zapasowej maszyny wirtualnej na nowej maszynie wirtualnej
Sprawdzanie poprawności (archiwum)	Sprawdzanie poprawności jednego archiwum
Sprawdzanie poprawności (kopia zapasowa)	Sprawdzanie poprawności kopii zapasowych
Sprawdzanie poprawności (skarbiec)	Sprawdzanie poprawności wszystkich archiwów przechowywanych w skarbcu
Czyszczenie	Usuwanie kopii zapasowych z archiwum kopii zapasowych zgodnie z regułami przechowywania
Tworzenie strefy ASZ	Tworzenie strefy Acronis Secure Zone
Zarządzanie strefą ASZ	Zmiana rozmiaru, zmiana hasła i usuwanie strefy Acronis Secure Zone
Zarządzanie dyskami	Operacje zarządzania dyskami
Kompaktowanie	Zadanie usługi wykonywane na węźle magazynowania
Indeksowanie	Zadanie deduplikacji wykonywane przez węzeł magazynowania w skarbcu po zakończeniu tworzenia kopii zapasowej

W zależności od typu zadania oraz od tego, czy zadanie jest uruchomione lub nie, jest wyświetlana kombinacja następujących kart:

Zadanie

Karta **Zadanie** jest identyczna dla wszystkich typów zadań. Zawiera ogólne informacje na temat wybranego zadania.

Archiwum

W przypadku zadań tworzenia kopii zapasowej, sprawdzania poprawności archiwum i czyszczenia dostępna jest karta **Archiwum**.

Zawiera ona informacje na temat archiwum: jego nazwę, typ, rozmiar, miejsce zapisania itp.

Kopia zapasowa

W przypadku zadań odzyskiwania, sprawdzania poprawności kopii zapasowej i eksportowania dostępna jest karta **Kopia zapasowa**.

Zawiera ona szczegółowe informacje na temat wybranej kopii zapasowej: datę jej utworzenia, typ (pełna, przyrostowa, różnicowa), informacje na temat archiwum i skarbca, w którym jest zapisana.

Ustawienia

Na karcie **Ustawienia** są dostępne informacje na temat planowania i opcji, których wartości są różne od domyślnych.

Postęp

Karta **Postęp** jest dostępna po uruchomieniu zadania. Jest ona taka sama dla różnych typów zadań. Zawiera informacje dotyczące postępu zadania, czasu jego wykonywania i innych parametrów.

Szczegóły planu tworzenia kopii zapasowych

Na czterech kartach okna **Szczegóły planu tworzenia kopii zapasowych** (zduplikowanego także w panelu **Informacja**) znajdują się wszystkie informacje dotyczące wybranego planu tworzenia kopii zapasowych.

Jeśli jedno z zadań planu wymaga działania użytkownika, w górnej części kart zostanie wyświetlony odpowiedni komunikat. Będzie on zawierał krótki opis problemu oraz przyciski czynności pozwalające wybrać odpowiednią czynność lub zatrzymać plan.

Plan tworzenia kopii zapasowych

Karta **Plan tworzenia kopii zapasowych** zawiera następujące informacje ogólne na temat wybranego planu:

- **Nazwa** — nazwa planu tworzenia kopii zapasowych.
- **Origin** (Pochodzenie) — określa, czy plan został utworzony na komputerze zarządzanym przy użyciu funkcji zarządzania bezpośredniego (pochodzenie lokalne), czy też pojawił się na komputerze jako wynik wdrożenia zasad tworzenia kopii zapasowych z serwera zarządzania (pochodzenie centralne).
- **Zasady** (w przypadku planów tworzenia kopii zapasowych mających pochodzenie centralne) — nazwa zasad tworzenia kopii zapasowych, których wdrożenie spowodowało utworzenie planu tworzenia kopii zapasowych.
- **Konto** — nazwa konta, na którym uruchamia się plan.
- **Właściciel** — nazwa użytkownika, który utworzył lub jako ostatni zmodyfikował plan.
- **Stan** — stan wykonania (s. 205) planu tworzenia kopii zapasowych.
- **Status** — status (s. 206) planu tworzenia kopii zapasowych.
- **Harmonogram** — określa, czy zadanie jest zaplanowane, czy też skonfigurowane na potrzeby uruchamiania ręcznego.
- **Ostatnia kopia zapasowa** — czas od ostatniego utworzenia kopii zapasowej.

- **Creation** (Utworzenie) — data utworzenia planu tworzenia kopii zapasowych.
- **Komentarze** — opis planu (jeśli dostał dostarczony).

Źródło

Karta **Źródło** zawiera następujące informacje na temat danych wybranych do utworzenia kopii zapasowej:

- **Typ źródła** — typ danych (s. 224) wybranych do utworzenia kopii zapasowej.
- **Elementy uwzględniane w kopii zapasowej** — elementy wybrane do utworzenia kopii zapasowej i ich rozmiar.

Miejsce docelowe

Karta **Miejsce docelowe** zawiera następujące informacje:

- **Lokalizacja** — nazwa skarbca lub ścieżka do folderu, w którym jest przechowywane archiwum.
- **Nazwa archiwum** — nazwa archiwum.
- **Komentarze dotyczące archiwum** — komentarze na temat archiwum (jeśli zostały dostarczone).

Ustawienia

Karta **Ustawienia** zawiera następujące informacje:

- **Schemat tworzenia kopii zapasowych** — wybrany schemat tworzenia kopii zapasowych i wszystkie jego ustawienia z harmonogramami.
- **Sprawdzanie poprawności** (jeśli zostało wybrane) — zdarzenia poprzedzające lub następujące po sprawdzaniu poprawności oraz harmonogram sprawdzania poprawności.
- **Opcje tworzenia kopii zapasowej** — opcje tworzenia kopii zapasowych zmienione w porównaniu z wartościami domyślnymi.

6.1.3 Dziennik

Dziennik zawiera historię operacji wykonywanych przez program Acronis Backup & Recovery 10 na komputerze lub czynności wykonywanych przez użytkownika na komputerze przy użyciu programu. Gdy użytkownik na przykład edytuje zadanie, do dziennika jest dodawany odpowiedni wpis. Gdy program wykonuje zadanie, dodaje wiele wpisów. Korzystając z dziennika, można sprawdzać operacje oraz wyniki wykonywania zadań, w tym również przyczyny niepowodzeń (jeśli wystąpiły).

Sposób pracy z wpisami dziennika

- Aby wyświetlić żądane wpisy dziennika, należy użyć filtrów. Można również ukrywać niepotrzebne kolumny i wyświetlać ukryte. Aby uzyskać szczegółowe informacje, zobacz sekcję Filtrowanie i sortowanie wpisów dziennika (s. 218).
- W tabeli dziennika należy wybrać wpis dziennika (lub wpisy dziennika), aby wykonać związaną z nim czynność. Aby uzyskać szczegółowe informacje, zobacz Czynności dotyczące wpisów dziennika (s. 217).
- Panel **Informacja** służy do przeglądania szczegółowych informacji na temat wybranego wpisu dziennika. Panel jest domyślnie zwinięty. Aby rozwinąć panel, należy kliknąć przycisk  . Zawartość panelu jest także zduplikowana w oknie **Szczegóły wpisu dziennika** (s. 218).

Otwieranie widoku Dziennik zawierającego wstępnie odfiltrowane wpisy dziennika

Po wybraniu elementów w innych widokach administracyjnych (**Pulpit nawigacyjny**, **Plany i zadania tworzenia kopii zapasowych**) można wyświetlić widok **Dziennik**, zawierający wpisy odfiltrowane

wstępnie pod kątem sprawdzanego elementu. Dlatego nie trzeba samemu konfigurować filtrów w tabeli dziennika.

Widok	Czynność
Pulpit nawigacyjny	Kliknij prawym przyciskiem myszy dowolną podświetloną datę w kalendarzu i wybierz **Wyświetl dziennik**. Wyświetlony widok **Dziennik** będzie zawierał listę wpisów przefiltrowaną według wybranej daty.
Plany i zadania tworzenia kopii zapasowych	Wybierz plan tworzenia kopii zapasowych lub zadanie, a następnie kliknij **Wyświetl dziennik**. Wyświetlony widok Dziennik będzie zawierał listę wpisów związanych z wybranym planem lub zadaniem.

Czynności dotyczące wpisów dziennika

Wszystkie opisane poniżej operacje wykonuje się, klikając odpowiednie elementy na **pasku narzędzi** dziennika. Wszystkie te operacje można również wykonać za pomocą menu kontekstowego (klikając prawym przyciskiem myszy wpis dziennika) lub za pomocą paska **Log actions** (Czynności dotyczące dziennika) (w panelu **Czynności i narzędzia**).

Poniżej przedstawiono wytyczne dotyczące wykonywania czynności związanych z wpisami dziennika.

Zadanie	Działanie
Wybierz pojedynczy wpis dziennika	Kliknij wpis.
Wybierz wiele wpisów dziennika	▪ *Niesąsiadujące*: przytrzymaj naciśnięty klawisz **CTRL** i kliknij pojedynczo wpisy dziennika. ▪ *Sąsiadujące*: wybierz pojedynczy wpis dziennika, a następnie przytrzymaj naciśnięty klawisz **SHIFT** i kliknij inny wpis. Wszystkie wpisy między pierwszym a ostatnim zaznaczeniem także zostaną zaznaczone.
Wyświetl szczegółowe informacje o wpisie dziennika	1. Wybierz wpis dziennika. 2. Wykonaj jedną z następujących czynności: ▪ Kliknij **Wyświetl szczegóły**. W oddzielnym oknie zostaną wyświetlone szczegółowe informacje o wpisie dziennika. ▪ Rozwiń panel Informacja, klikając przycisk.
Zapisz wybrane wpisy dziennika w pliku	1. Zaznacz pojedynczy wpis dziennika lub wiele wpisów dziennika. 2. Kliknij **Zapisz zaznaczone w pliku**. 3. W otwartym oknie określ ścieżkę i nazwę pliku.
Zapisz wszystkie wpisy dziennika w pliku	1. Upewnij się, że nie są ustawione żadne filtry. 2. Kliknij **Zapisz wszystko w pliku**. 3. W otwartym oknie określ ścieżkę i nazwę pliku.
Zapisz wszystkie odfiltrowane wpisy dziennika w pliku	1. Ustaw filtry tak, aby uzyskać listę wpisów dziennika spełniających kryteria filtrowania. 2. Kliknij **Zapisz wszystko w pliku**. 3. W otwartym oknie określ ścieżkę i nazwę pliku. Wpisy dziennika z tej listy zostaną zapisane.

Usuń wszystkie wpisy dziennika	Kliknij **Wyczyść dziennik**. Wszystkie wpisy dziennika zostaną usunięte z dziennika i zostanie utworzony nowy wpis dziennika. Będzie on zawierał informacje o tym, kto i kiedy usunął wpisy.

Filtrowanie i sortowanie wpisów dziennika

Poniżej przedstawiono wytyczne dotyczące filtrowania i sortowania wpisów dziennika.

Zadanie	Działanie
Wyświetl wpisy dziennika dotyczące określonego przedziału czasu	1. W polu **Od** wybierz datę, od której mają być wyświetlane wpisy dziennika. 2. W polu **Do** wybierz datę, do której mają być wyświetlane wpisy dziennika.
Filtruj wpisy dziennika według typu	Naciśnij lub zwolnij następujące przyciski paska narzędzi: aby filtrować komunikaty o błędach, aby filtrować komunikaty ostrzegawcze, aby filtrować komunikaty informacyjne.
Filtruj wpisy dziennika według oryginalnego planu tworzenia kopii zapasowych lub typu jednostki zarządzanej	W kolumnie **Plan tworzenia kopii zapasowych** (lub **Typ jednostki zarządzanej**) wybierz z listy plan tworzenia kopii zapasowych lub typ jednostki zarządzanej.
Filtruj wpisy dziennika według zadania, jednostki zarządzanej, komputera, kodu, właściciela	W polu pod odpowiednim nagłówkiem kolumny wpisz wymaganą wartość (nazwę zadania, nazwę komputera, nazwę właściciela itp.). Zostanie wyświetlona lista wpisów dziennika, które całkowicie lub częściowo zgadzają się z wprowadzoną wartością.
Sortuj wpisy dziennika według daty i godziny	Kliknij nagłówek kolumny, aby posortować wpisy dziennika w porządku rosnącym. Kliknij go ponownie, aby posortować wpisy dziennika w porządku malejącym.

Konfigurowanie tabeli dziennika

Domyślnie w tabeli jest wyświetlanych siedem kolumn, a pozostałe są ukryte. W razie potrzeby można ukryć wyświetlane kolumny i wyświetlić ukryte kolumny.

Aby wyświetlić lub ukryć kolumny

1. Kliknij prawym przyciskiem myszy nagłówek kolumny, aby wyświetlić menu kontekstowe. Zaznaczone elementy menu odpowiadają nagłówkom kolumn wyświetlanych w tabeli.
2. Kliknij elementy, które chcesz wyświetlić/ukryć.

Szczegóły wpisu dziennika

Wyświetlane są szczegółowe informacje dotyczące wpisu dziennika. Informacje te można skopiować do schowka.

Aby skopiować szczegółowe informacje, kliknij przycisk **Kopiuj do schowka**.

Pola danych wpisu dziennika

Wpis lokalnego dziennika zawiera następujące pola danych:

- **Typ** — typ zdarzenia (Błąd, Ostrzeżenie, Informacja);

- **Data** — data i godzina wystąpienia zdarzenia;
- **Plan tworzenia kopii zapasowych** — plan tworzenia kopii zapasowych, z którym związane jest zdarzenie (jeśli dotyczy);
- **Zadanie** — zadanie, z którym związane jest zdarzenie (jeśli dotyczy);
- **Kod** —kod programu dotyczący zdarzenia. Każdy typ zdarzenia w programie ma własny kod. Kod to liczba całkowita, która może zostać użyta przez usługę pomocy technicznej Acronis w celu rozwiązania problemu;
- **Moduł** — numer modułu programu, w którym wystąpiło zdarzenie. Jest to liczba całkowita, która może zostać użyta przez usługę pomocy technicznej Acronis w celu rozwiązania problemu;
- **Właściciel** — nazwa użytkownika będącego właścicielem planu tworzenia kopii zapasowych (tylko w systemie operacyjnym);
- **Komunikat** — tekstowy opis zdarzenia.

Kopiowane szczegóły wpisu dziennika będą miały następujący wygląd:

```
-------------------------Szczegóły wpisu dziennika--------------------------
Typ:                                Informacja
Data i godzina:                     DD.MM.RRRR HH:MM:SS
Plan tworzenia kopii zapasowych:    Nazwa planu tworzenia kopii zapasowych
Zadanie:                            Nazwa zadania
Komunikat:                          Opis operacji
Kod:                                12(3x45678A)
Moduł:                              Nazwa modułu
Właściciel:                         Właściciel planu
----------------------------------------------------------------------------
```

Sposób wyświetlania daty i godziny zależy od ustawień lokalnych.

6.2 Tworzenie planu tworzenia kopii zapasowych

Przed utworzeniem pierwszego planu tworzenia kopii zapasowych (s. 425) zapoznaj się z podstawowymi pojęciami (s. 30) stosowanymi w programie Acronis Backup & Recovery 10.

Aby utworzyć plan tworzenia kopii zapasowych, wykonaj poniższe czynności.

Ogólne

Nazwa planu

[Opcjonalnie] Wprowadź unikatową nazwę planu tworzenia kopii zapasowych. Dobrze dobrana nazwa umożliwi jego identyfikację pośród innych planów.

Poświadczenia planu (s. 222)

[Opcjonalnie] Plan tworzenia kopii zapasowych będzie uruchamiany w imieniu użytkownika, który go utworzył. W razie potrzeby można zmienić poświadczenia konta planu. Aby uzyskać dostęp do tej opcji, zaznacz pole wyboru **Widok zaawansowany**.

Komentarze

[Opcjonalnie] Wpisz opis planu tworzenia kopii zapasowych. Aby uzyskać dostęp do tej opcji, zaznacz pole wyboru **Widok zaawansowany**.

Etykieta (s. 222)

[Opcjonalnie] Wpisz etykietę tekstową dla komputera, którego kopię zapasową chcesz utworzyć. Etykieta umożliwia identyfikację komputera w różnych scenariuszach. Aby uzyskać dostęp do tej opcji, zaznacz pole wyboru **Widok zaawansowany**.

Elementy uwzględniane w kopii zapasowej

Typ źródła (s. 224)

Wybierz typ danych przeznaczonych do kopii zapasowej. Typ danych zależy od agentów zainstalowanych na komputerze.

Elementy uwzględniane w kopii zapasowej (s. 225)

Określ elementy danych przeznaczone do kopii zapasowej. Lista elementów kopii zapasowej zależy od określonego uprzednio typu danych.

Poświadczenia dostępu (s. 227)

[Opcjonalnie] Jeśli konto planu nie ma uprawnień dostępu do danych źródłowych, podaj poświadczenia dla danych. Aby uzyskać dostęp do tej opcji, zaznacz pole wyboru **Widok zaawansowany**.

Wykluczenia (s. 228)

[Opcjonalnie] Skonfiguruj wykluczenia, określając konkretne typy plików, które nie powinny znaleźć się w kopii zapasowej. Aby uzyskać dostęp do tej opcji, zaznacz pole wyboru **Widok zaawansowany**.

Miejsce docelowe kopii zapasowej

Archiwum (s. 229)

Określ ścieżkę do lokalizacji, w której przechowywane będzie archiwum kopii zapasowej, oraz nazwę archiwum. Zaleca się, aby nazwa archiwum była unikatowa w danej lokalizacji. Domyślna nazwa to Archiwum(N), gdzie N to kolejny numer archiwum w wybranej lokalizacji.

Plikom kopii zapasowej nadawaj nazwy archiwum występujące w programie Acronis True Image Echo, a nie nazwy wygenerowane automatycznie.

Opcja niedostępna w przypadku tworzenia kopii zapasowej w skarbcu zarządzanym, na taśmie, w strefie Acronis Secure Zone lub w magazynie Acronis Online Backup Storage.

[Opcjonalnie] Zaznacz to pole wyboru, jeśli chcesz używać uproszczonego nazewnictwa dla kopii zapasowych archiwum.

Poświadczenia dostępu (s. 235)

[Opcjonalnie] Jeśli konto planu nie ma uprawnień dostępu do lokalizacji, podaj związane z nią poświadczenia. Aby uzyskać dostęp do tej opcji, zaznacz pole wyboru **Widok zaawansowany**.

Komentarze dotyczące archiwum

[Opcjonalnie] Wprowadź komentarze do archiwum. Aby uzyskać dostęp do tej opcji, zaznacz pole wyboru **Widok zaawansowany**.

Sposób tworzenia kopii zapasowej

Schemat tworzenia kopii zapasowych (s. 236)

Określ czas i częstotliwość tworzenia kopii zapasowych danych, zdefiniuj okres przechowywania utworzonych archiwów kopii zapasowych w wybranej lokalizacji oraz ustal harmonogram procedury czyszczenia archiwum. Skorzystaj z dobrze znanych, zoptymalizowanych schematów tworzenia kopii zapasowych, takich jak Dziadek-ojciec-syn i Wieża Hanoi, zdefiniuj schemat niestandardowy lub utwórz kopię zapasową danych jeden raz.

Sprawdzanie poprawności archiwum

Czas sprawdzania poprawności (s. 246)

[Opcjonalnie] Zdefiniuj czas i częstotliwość sprawdzania poprawności oraz czy ma być sprawdzana poprawność całego archiwum, czy ostatniej kopii zapasowej w tym archiwum.

Opcje tworzenia kopii zapasowych

Ustawienia

[Opcjonalnie] Skonfiguruj parametry operacji tworzenia kopii zapasowej, takie jak polecenia poprzedzające/następujące po tworzeniu kopii, maksymalna przepustowość sieci przydzielona do strumienia kopii zapasowej lub stopień kompresji archiwum. Jeśli w tej sekcji nie wykonasz żadnej czynności, zostaną użyte wartości domyślne (s. 109).

Po zmianie dowolnego z ustawień na wartość różną od domyślnej pojawi się nowy wiersz zawierający nowo skonfigurowaną wartość. Stan ustawienia zmieni się z wartości **Domyślne** na **Niestandardowe**. W razie ponownej zmiany ustawienia w wierszu pojawi się nowa wartość, o ile nie będzie to wartość domyślna. W przypadku wartości domyślnej wiersz zniknie. Dlatego w tej sekcji strony **Utwórz plan tworzenia kopii zapasowych** zawsze wyświetlane są tylko ustawienia różne od domyślnych.

Aby przywrócić wartości domyślne wszystkich ustawień, kliknij **Przywróć domyślne**.

Konwertuj na maszynę wirtualną

Dotyczy kopii zapasowych **dysku/woluminu**, **całych maszyn wirtualnych** lub **woluminów maszyny wirtualnej**.

Opcja niedostępna na komputerach z systemem Linux.

Skonfigurowanie regularnej konwersji pozwala uzyskać kopię serwera lub stacji roboczej na maszynie wirtualnej, którą można szybko włączyć w przypadku awarii oryginalnego komputera. Konwersję można wykonać za pomocą tego samego agenta, który wykonuje kopię zapasową, lub za pomocą agenta zainstalowanego na innym komputerze. W tym drugim przypadku archiwum należy przechowywać w lokalizacji udostępnionej, takiej jak folder sieciowy lub skarbiec zarządzany. Dzięki temu drugi komputer będzie miał dostęp do archiwum.

Czas przeprowadzenia konwersji (s. 247)

[Opcjonalnie] Określ, czy należy konwertować każdą pełną, przyrostową lub różnicową kopię zapasową, czy ostatnią utworzoną kopię zapasową według harmonogramu. W razie potrzeby określ harmonogram konwersji.

Host (s. 247)

Określ komputer, który wykona konwersję. Na komputerze musi być zainstalowany Acronis Backup & Recovery 10 Agent dla systemu Windows, Agent dla ESX/ESXi lub Agent dla Hyper-V.

Serwer wirtualizacji (s. 247)

W tym miejscu można wybrać typ i lokalizację wynikowej maszyny wirtualnej. Dostępne opcje zależą od hosta wybranego w poprzednim kroku.

Magazyn (s. 247)

Wybierz magazyn na serwerze wirtualizacji lub folder, w którym zostaną umieszczone pliki maszyny wirtualnej.

Wynikowe maszyny wirtualne

Określ nazwę maszyny wirtualnej.

Po wykonaniu wszystkich wymaganych czynności kliknij **OK**, aby utworzyć plan tworzenia kopii zapasowych.

Następnie może pojawić się monit o podanie hasła (s. 222).

Utworzony plan będzie dostępny do sprawdzenia i zarządzania w widoku **Plany i zadania tworzenia kopii zapasowych** (s. 205).

6.2.1 Dlaczego program wyświetla monit o hasło?

Zaplanowane lub przełożone zadanie musi zostać uruchomione niezależnie od zalogowanych użytkowników. W sytuacji, gdy nie określono wprost poświadczeń, z którymi zadania mają zostać uruchomione, program zaproponuje użycie konta użytkownika. Wprowadź hasło użytkownika, określ inne konto lub zmień typ zaplanowanego uruchomienia na ręczny.

6.2.2 Poświadczenia planu tworzenia kopii zapasowych

Podaj poświadczenia konta, na którym zadania planu będą wykonywane.

Aby określić poświadczenia

1. Wybierz jedno z następujących ustawień:
   - **Użyj poświadczeń bieżącego użytkownika**

     Zadania będą uruchamiane przy użyciu poświadczeń, z którymi zalogował się użytkownik rozpoczynający zadania. Jeśli jedno z zadań ma zostać wykonane według harmonogramu, w momencie zakończenia tworzenia planu użytkownik zostanie poproszony o aktualne hasło użytkownika.
   - **Użyj następujących poświadczeń**

     Zadania będą zawsze uruchamiane przy użyciu poświadczeń określonych przez użytkownika, niezależnie od tego, czy zadanie będzie uruchamiane ręcznie, czy wykonywane według harmonogramu.

     Określ:
     - **Nazwa użytkownika**. Wprowadzając nazwę konta użytkownika usługi Active Directory, należy określić również nazwę domeny (DOMENA\Nazwa_użytkownika lub Nazwa_użytkownika@domena).
     - **Hasło**. Hasło dla konta.
2. Kliknij **OK**.

Aby dowiedzieć się więcej na temat operacji użytkowników z różnymi uprawnieniami, zobacz sekcję Uprawnienia użytkowników na zarządzanym komputerze (s. 34).

6.2.3 Etykieta (zachowanie właściwości komputera w kopii zapasowej)

Podczas każdego tworzenia kopii zapasowej danych na komputerze do kopii zapasowej są dołączane informacje na temat nazwy komputera, systemu operacyjnego, pakietu Service Pack systemu Windows i identyfikatora zabezpieczeń (SID) oraz etykieta tekstowa zdefiniowana przez użytkownika. Etykieta może zawierać nazwę działu lub nazwisko właściciela komputera, albo podobne informacje, których można użyć jako znacznika lub klucza.

W przypadku odzyskiwania komputera na serwerze VMware ESX Server przy użyciu Agenta dla ESX/ESXi albo konwertowania (s. 247) kopii zapasowej na maszynę wirtualną ESX/ESXi te właściwości zostaną przeniesione do konfiguracji maszyny wirtualnej. Możesz je wyświetlić w ustawieniach maszyny wirtualnej: **Edytuj ustawienia** > **Opcje** > **Zaawansowane** > **Ogólne** > **Parametry konfiguracji**. Przy użyciu tych niestandardowych parametrów możesz wybierać, sortować i łączyć w grupy maszyny wirtualne. Może to być przydatne w różnych scenariuszach.

Przykład:

Przyjmijmy, że migrujesz swoje biuro lub centrum danych do środowiska wirtualnego. Przy użyciu oprogramowania innych firm, które może uzyskiwać dostęp do parametrów konfiguracji przy użyciu interfejsu VMware API, możesz automatycznie stosować zasady zabezpieczeń na każdym komputerze, nawet przed jego włączeniem.

Aby dodać etykietę tekstową do kopii zapasowej:

1. Na stronie **Utwórz plan tworzenia kopii zapasowych** (s. 219) lub **Utwórz zasady tworzenia kopii zapasowych** (s. 395) zaznacz pole wyboru **Widok zaawansowany**.
2. W polu **Etykieta** wprowadź etykietę tekstową lub wybierz ją z menu rozwijanego.

Omówienie parametrów

Parametr	Wartość	Opis
acronisTag.label	<string>	Etykieta zdefiniowana przez użytkownika. Etykietę może ustawić użytkownik podczas tworzenia planu lub zasad tworzenia kopii zapasowych.
acronisTag.hostname	<string>	Nazwa hosta (w pełni kwalifikowana nazwa domeny, FQDN)
acronisTag.os.type	<string>	System operacyjny,
acronisTag.os.servicepack	0, 1, 2...	Wersja dodatku Service Pack zainstalowanego w systemie. Tylko dla systemu operacyjnego Windows.
acronisTag.os.sid	<string>	Identyfikator zabezpieczeń (SID) komputera Na przykład: S-1-5-21-874133492-782267321-3928949834. Tylko dla systemu operacyjnego Windows.

Wartości parametru „acronisTag.os.type”

Windows NT 4	winNTGuest
Windows 2000 Professional	win2000ProGuest
Windows 2000 Server	win2000ServGuest
Windows 2000 Advanced Server	win2000ServGuest
Windows XP — wszystkie wersje	winXPProGuest
Windows XP — wszystkie wersje (64-bitowe)	winXPPro64Guest
Windows Server 2003 — wszystkie wersje	winNetStandardGuest
Windows Server 2003 — wszystkie wersje (64-bitowe)	winNetStandard64Guest
Windows 2008	winLonghornGuest
Windows 2008 (64-bitowy)	winLonghorn64Guest
Windows Vista	winVistaGuest
Windows Vista (64-bitowy)	winVista64Guest
Windows 7	windows7Guest
Windows 7 (64-bitowy)	windows7_64Guest
Windows Server 2008 R2 (64-bitowy)	windows7Server64Guest
Linux	otherLinuxGuest

Linux (64-bitowy)	otherLinux64Guest
Inny system operacyjny	otherGuest
Inny system operacyjny (64-bitowy)	otherGuest64

Przykład

acronisTag.label = “DEPT:BUCH; COMP:SUPERSERVER; OWNER:EJONSON”

acronisTag.hostname = “superserver.corp.local”

acronisTag.os.type = “windows7Server64Guest”

acronisTag.os.servicepack = “1”

acronisTag.os.sid = “S-1-5-21-874133492-782267321-3928949834”

6.2.4 Typ źródła

Wybierz typ danych, których kopię zapasową chcesz utworzyć na zarządzanym komputerze. Lista dostępnych typów danych zależy od agentów zarządzających na komputerze:

Pliki

Opcja dostępna, gdy jest zainstalowany Acronis Backup & Recovery 10 Agent dla systemu Windows (lub dla systemu Linux).

Wybór tej opcji umożliwia utworzenie kopii zapasowej określonych plików i folderów.

Jeśli nie jest wymagana możliwość odzyskiwania systemu operacyjnego ze wszystkimi ustawieniami i aplikacjami, a jedynie bezpieczne przechowywanie tylko niektórych danych (na przykład bieżącego projektu), wybierz utworzenie kopii zapasowej plików. Zmniejszy to rozmiar archiwum, oszczędzając przy tym miejsce w magazynie.

Dyski/woluminy

Opcja dostępna, gdy jest zainstalowany Acronis Backup & Recovery 10 Agent dla systemu Windows (lub dla systemu Linux).

Wybór tej opcji umożliwia utworzenie kopii zapasowej dysków i/lub woluminów. Aby tworzyć kopie zapasowe dysków lub woluminów, należy posiadać uprawnienia Administratora lub operatora kopii zapasowych.

Dzięki utworzeniu kopii zapasowej dysków i woluminów można odzyskać cały system w razie poważnego uszkodzenia danych lub awarii sprzętu. Procedura tworzenia kopii zapasowej jest szybsza niż operacja kopiowania plików, a może znacząco przyspieszyć proces tworzenia kopii zapasowej w przypadku dużych woluminów danych.

Uwaga dotycząca użytkowników systemu Linux: *Zalecamy odmontowanie wszystkich woluminów zawierających systemy plików bez funkcji księgowania, takie jak system ext2, przed utworzeniem ich kopii zapasowej. W przeciwnym przypadku po odzyskaniu woluminy te mogą zawierać uszkodzone pliki, a odzyskiwanie ze zmianą rozmiaru może zakończyć się niepowodzeniem.*

Wszystkie maszyny wirtualne

Dostępny, gdy zainstalowany jest agent Acronis Backup & Recovery 10 dla Hyper-V (lub ESX/ESXi).

Tę opcję należy wybrać, aby utworzyć kopię zapasową jednej lub kilku maszyn wirtualnych znajdujących się na serwerze wirtualizacji.

Utworzenie kopii zapasowej maszyny wirtualnej oznacza utworzenie kopii wszystkich dysków oraz konfiguracji maszyny. Ten typ źródła umożliwia tworzenie kopii zapasowych wielu maszyn. Jest to przydatne w przypadku, gdy istnieje duża liczba małych (pod kątem pojemności dysków wirtualnych) serwerów starszego typu, takich jak wynikające z konsolidacji obciążenia. Dla każdej maszyny tworzone jest osobne archiwum.

Woluminy maszyny wirtualnej

Dostępny, gdy zainstalowany jest agent Acronis Backup & Recovery 10 dla Hyper-V (lub ESX/ESXi).

Tę opcję należy wybrać, aby utworzyć kopię zapasową poszczególnych dysków lub woluminów maszyny wirtualnej znajdującej się na serwerze wirtualizacji.

Ten typ źródła umożliwia wybranie maszyny, a następnie wybranie dysków/woluminów, których kopię zapasową ma utworzyć program. Jest to przydatne, gdy system operacyjny i aplikacje, takie jak serwer bazy danych działają na dyskach wirtualnych, ale dane, takie jak bazy danych, są zapisywane na dyskach fizycznych o dużej pojemności dodanych do tej samej maszyny. Można użyć różnych strategii tworzenia kopii zapasowych dysków wirtualnych i pamięci fizycznej.

6.2.5 Elementy uwzględniane w kopii zapasowej

Elementy uwzględniane w kopii zapasowej zależą od typu źródła (s. 224) wybranego wcześniej.

Wybieranie dysków i woluminów

Aby określić dyski/woluminy przeznaczone do kopii zapasowej

1. Zaznacz pola wyboru przy dyskach i woluminach, które chcesz uwzględnić w kopii zapasowej. Można wybrać dowolny zestaw dysków i woluminów.

   Jeśli system operacyjny i jego program ładujący znajdują się na różnych woluminach, w kopii zapasowej należy zawsze uwzględnić oba woluminy. Woluminy muszą być również odzyskiwane wspólnie, gdyż w przeciwnym razie istnieje duże ryzyko, że system operacyjny nie uruchomi się.

   W systemie Linux woluminy logiczne i urządzenia MD są wyświetlane w sekcji **Dynamiczne i GPT**. Aby uzyskać więcej informacji na temat tworzenia kopii zapasowych takich woluminów i urządzeń, zobacz „Tworzenie kopii zapasowych woluminów LVM i urządzeń MD (Linux) (s. 50)”.
2. [Opcjonalnie] Aby utworzyć dokładną kopię dysku lub woluminu na poziomie fizycznym, zaznacz pole wyboru **Wykonaj kopię „sektor po sektorze”.** Wynikowa kopia zapasowa będzie tego samego rozmiaru co kopiowany dysk (jeśli **Stopień kompresji** ma ustawienie „**Brak**”). Operacja kopiowania „sektor po sektorze” pozwala tworzyć kopie zapasowe dysków zawierających nierozpoznane lub nieobsługiwane systemy plików oraz dane w innych zastrzeżonych formatach.
3. Kliknij **OK**.

Co zawiera kopia zapasowa dysku lub woluminu?

Gdy opcja kopiowania „sektor po sektorze” jest wyłączona, kopia zapasowa dysku lub woluminu z obsługiwanym systemem plików zawiera wyłącznie sektory z danymi. Zmniejsza to rozmiar wynikowej kopii zapasowej oraz przyspiesza operacje jej tworzenia i odzyskiwania danych.

Windows

Przy tworzeniu kopii zapasowej nie jest uwzględniany plik wymiany (pagefile.sys) ani plik z zawartością pamięci RAM komputera przechodzącego w stan hibernacji (hiberfil.sys). Po odzyskaniu danych pliki te zostaną ponownie utworzone w odpowiednim miejscu z zerowym rozmiarem.

Kopia zapasowa woluminu zawiera wszystkie pozostałe pliki i foldery wybranego woluminu niezależnie od ich atrybutów (w tym pliki ukryte i systemowe), rekord startowy, tablicę FAT (o ile istnieje), katalog główny i zerową ścieżkę dysku twardego z głównym rekordem rozruchowym (MBR). Przy tworzeniu kopii zapasowej nie jest uwzględniany kod startowy woluminów GPT.

Kopia zapasowa dysku zawiera wszystkie woluminy wybranego dysku (w tym woluminy ukryte, takie jak partycje konserwacyjne producenta) oraz ścieżkę zerową głównego rekordu rozruchowego.

Linux

Kopia zapasowa woluminu zawiera wszystkie pliki i foldery wybranego woluminu niezależnie od ich atrybutów, rekord startowy oraz superblok systemu plików.

Kopia zapasowa dysku zawiera wszystkie woluminy dysku oraz ścieżkę zerową z głównym rekordem rozruchowym.

Wybieranie plików i folderów

Aby wybrać pliki i foldery do kopii zapasowej

1. Rozwiń elementy drzewa folderów lokalnych, aby wyświetlić ich foldery i pliki zagnieżdżone.
2. Wybierz element, zaznaczając odpowiednie pole wyboru w drzewie. Zaznaczenie pola wyboru przypisanego do folderu oznacza, że cała jego zawartość (pliki i foldery) zostanie uwzględniona w kopii zapasowej. Będzie to dotyczyło również nowych plików, które pojawią się w nim w przyszłości.

   Kopia zapasowa na poziomie plików nie jest wystarczająca do odzyskania systemu operacyjnego. Aby umożliwić odzyskanie systemu operacyjnego, trzeba wykonać kopię zapasową dysku.

   Użyj tabeli w prawej części okna, aby przejrzeć i wybrać elementy zagnieżdżone. Zaznaczenie pola wyboru obok nagłówka kolumny **Nazwa** powoduje automatyczne zaznaczenie wszystkich elementów w tabeli. Wyczyszczenie tego pola wyboru powoduje automatyczne usunięcie zaznaczenia dla wszystkich elementów.
3. Kliknij **OK**.

Wybór całych maszyn wirtualnych

Tworzenie kopii zapasowej maszyny wirtualnej oznacza tworzenie kopii zapasowej wszystkich dysków tej maszyny oraz jej konfiguracji.

Aby utworzyć kopię zapasową jednego lub więcej maszyn wirtualnych znajdujących się na serwerze wirtualizacji

1. Zaznacz pola wyboru obok maszyn wirtualnych, których kopie zapasowe chcesz utworzyć. Zaznaczenie pola wyboru dotyczącego serwera wirtualizacji spowoduje automatyczne zaznaczenie wszystkich maszyn wirtualnych na tym serwerze.

   W prawej części okna można wyświetlić szczegóły dotyczące wybranych maszyn wirtualnych lub wybranego serwera wirtualizacji.
2. Kliknij **OK**.

W wyniku operacji utworzenia kopii zapasowej całej maszyny wirtualnej powstaje standardowa kopia zapasowa dysku (s. 424). W przypadku korzystania z agenta Acronis Backup & Recovery 10 Agent dla systemu Windows lub dla systemu Linux można zamontować woluminy kopii zapasowej, odzyskać z niej poszczególne pliki oraz odzyskać dyski i woluminy na komputer fizyczny. Podczas odzyskiwania zawartości kopii zapasowej na nową maszynę wirtualną zostanie domyślnie wybrana konfiguracja maszyny wirtualnej przechowywana w tej kopii zapasowej.

Ograniczenia

Z hosta nie można utworzyć kopii zapasowej maszyny wirtualnej Hyper-V korzystającej z przynajmniej jednego dysku z przekazywaniem (dysku fizycznego, lokalnego lub SAN-LUN dołączonego do maszyny wirtualnej). Aby utworzyć kopię zapasową takiej maszyny lub jej dysków, na komputerze należy zainstalować agenta dla systemu Windows lub agenta dla systemu Linux.

Z hosta nie można utworzyć kopii zapasowej dysku SAN-LUN dołączonego do maszyny wirtualnej ESX/ESXi w trybie „kompatybilności fizycznej", jeśli maszyna jest uruchomiona (jest online). Aby utworzyć kopię zapasową takiego dysku, należy zatrzymać maszynę lub zainstalować na niej agenta dla systemu Windows lub agenta dla systemu Linux.

Wybór dysków i woluminów maszyny wirtualnej

Aby utworzyć kopię zapasową poszczególnych dysków lub woluminów maszyny wirtualnej znajdującej się na serwerze wirtualizacji

1. Wybierz maszynę wirtualną, dla której woluminów chcesz utworzyć kopię zapasową.

   W prawej części okna można wyświetlić szczegóły dotyczące wybranej maszyny wirtualnej.
2. Kliknij **OK**.
3. W oknie **Wybór dysków i woluminów** (s. 225) wybierz dyski lub woluminy maszyny wirtualnej. Tworzenie kopii zapasowej woluminów maszyny wirtualnej przypomina tworzenie kopii zapasowej woluminów komputera fizycznego. Zostanie również utworzona kopia zapasowa konfiguracji maszyny wirtualnej.

W wyniku operacji utworzenia kopii zapasowej woluminów maszyny wirtualnej powstaje standardowa kopia zapasowa dysku (s. 424). W przypadku korzystania z agenta Acronis Backup & Recovery 10 Agent dla systemu Windows lub dla systemu Linux można zamontować woluminy kopii zapasowej, odzyskać z niej poszczególne pliki oraz odzyskać dyski i woluminy na komputer fizyczny. Podczas odzyskiwania zawartości kopii zapasowej na nową maszynę wirtualną zostanie domyślnie wybrana konfiguracja maszyny wirtualnej przechowywana w tej kopii zapasowej.

Ograniczenia

Z hosta nie można utworzyć kopii zapasowej maszyny wirtualnej Hyper-V korzystającej z przynajmniej jednego dysku z przekazywaniem (dysku fizycznego, lokalnego lub SAN-LUN dołączonego do maszyny wirtualnej). Aby utworzyć kopię zapasową takiej maszyny lub jej dysków, na komputerze należy zainstalować agenta dla systemu Windows lub agenta dla systemu Linux.

Z hosta nie można utworzyć kopii zapasowej dysku SAN-LUN dołączonego do maszyny wirtualnej ESX/ESXi w trybie „kompatybilności fizycznej", jeśli maszyna jest uruchomiona (jest online). Aby utworzyć kopię zapasową takiego dysku, należy zatrzymać maszynę lub zainstalować na niej agenta dla systemu Windows lub agenta dla systemu Linux.

6.2.6 Poświadczenia dostępu do źródła

Określ poświadczenia wymagane w celu dostępu do danych, które zostaną uwzględnione w kopii zapasowej.

Aby określić poświadczenia

1. Wybierz jedną z następujących opcji:
   - **Użyj poświadczeń planu**

     Program uzyska dostęp do danych źródłowych przy użyciu poświadczeń konta planu tworzenia kopii zapasowych określonych w sekcji Ogólne.

- **Użyj następujących poświadczeń**

  Program uzyska dostęp do danych źródłowych przy użyciu określonych poświadczeń. Użyj tej opcji, jeśli konto planu nie posiada uprawnień dostępu do danych.

  Określ:

  - **Nazwa użytkownika**. Wprowadzając nazwę konta użytkownika usługi Active Directory, należy określić również nazwę domeny (DOMENA\Nazwa_użytkownika lub Nazwa_użytkownika@domena).
  - **Hasło**. Hasło dla konta.

2. Kliknij **OK**.

6.2.7 Wykluczenia

Skonfiguruj wykluczenia, określając konkretne typy plików nie uwzględnianych w kopii zapasowej. Z przechowywania w archiwum można wykluczyć na przykład bazę danych, pliki i foldery ukryte oraz systemowe, a także pliki z określonymi rozszerzeniami.

Aby określić pliki i foldery do wykluczenia:

Skonfiguruj dowolne z następujących parametrów:

- **Wyklucz wszystkie ukryte pliki i foldery**

  Opcja ta działa tylko w systemach plików obsługiwanych przez system Windows. Zaznacz to pole wyboru, aby pominąć pliki i foldery z atrybutem **Ukryty**. Jeśli folder jest **ukryty**, program wykluczy całą jego zawartość, w tym również pliki, które nie mają atrybutu **Ukryty**.

- **Wyklucz wszystkie pliki i foldery systemowe**

  Opcja ta działa tylko w systemach plików obsługiwanych przez system Windows. Zaznacz to pole wyboru, aby pominąć pliki i foldery z atrybutem **Systemowy**. Jeśli folder jest **systemowy**, program wykluczy całą jego zawartość, w tym również pliki, które nie mają atrybutu **Systemowy**.

*Atrybuty plików i folderów można sprawdzić w ich właściwościach lub używając polecenia **attrib**. Więcej informacji można znaleźć w Centrum pomocy i obsługi technicznej w systemie Windows.*

- **Wyklucz pliki spełniające następujące kryteria**

  Zaznacz to pole wyboru, aby pominąć pliki i foldery, których nazwy pasują do podanych na liście kryteriów zwanych maskami plików. Aby utworzyć listę masek plików, użyj przycisków **Dodaj**, **Edytuj**, **Usuń** i **Usuń wszystko**.

  W masce plików można użyć jednego lub kilku symboli wieloznacznych * i ?:

  Gwiazdka (*) zastępuje dowolną liczbę znaków w nazwie pliku (w tym również zero). Na przykład maska Dok*.txt zwraca pliki takie jak Dok.txt i Dokument.txt.

  Znak zapytania (?) zastępuje dokładnie jeden znak w nazwie pliku. Na przykład maska Dok?.txt zwraca pliki takie jak Dok1.txt i Doku.txt, ale nie zwraca plików Dok.txt ani Dok11.txt.

Aby wykluczyć folder określony przez ścieżkę zawierającą literę dysku, dodaj ukośnik odwrotny (\) do nazwy folderu w kryterium, np.: C:\Finanse\

Przykłady wykluczeń

Kryterium	Przykład	Opis
Windows i Linux		
Według nazwy	F.log F	Wyklucza wszystkie pliki o nazwie „F.log”. Wyklucza wszystkie foldery o nazwie „F”.
Według maski (*)	*.log F*	Wyklucza wszystkie pliki z rozszerzeniem .log. Wyklucza wszystkie pliki i foldery, których nazwa rozpoczyna się od litery „F” (np. foldery F, F1 i pliki F.log, F1.log).
Według maski (?)	F???.log	Wyklucza wszystkie pliki z rozszerzeniem .log, których nazwy składają się z czterech znaków i zaczynają od litery „F”.
Windows		
Według ścieżki pliku	C:\Finanse\F.log	Wyklucza plik „F.log” znajdujący się w folderze C:\Finanse.
Według ścieżki folderu	C:\Finanse\F\	Wyklucza folder C:\Finanse\F (należy określić pełną ścieżkę, rozpoczynającą się od litery dysku).
Linux		
Według ścieżki pliku	/home/user/Finanse/F.log	Wyklucza plik „F.log” znajdujący się w folderze /home/user/Finanse.
Według ścieżki folderu	/home/user/Finanse/	Wyklucza folder /home/user/Finanse.

6.2.8 Archiwum

Określ miejsce przechowywania i nazwę archiwum.

1. Wybieranie lokalizacji docelowej

Wprowadź pełną ścieżkę do lokalizacji docelowej w polu **Ścieżka** lub wybierz pożądaną lokalizację docelową w drzewie folderów.

- Aby utworzyć kopię zapasową danych w magazynie Acronis Online Backup Storage, kliknij **Zaloguj** i określ poświadczenia logowania do magazynu online. Następnie rozwiń grupę **Magazyn kopii zapasowych online** i wybierz konto.

  Przed utworzeniem kopii zapasowej w magazynie online należy zakupić subskrypcję usługi tworzenia kopii zapasowych online oraz aktywować tę subskrypcję na komputerach, których kopię zapasową chcesz utworzyć. Opcja tworzenia kopii zapasowej online jest niedostępna w systemie Linux i podczas pracy z nośnikiem startowym.

  Usługa Acronis Backup & Recovery 10 Online nie jest dostępna we wszystkich regionach. Aby uzyskać więcej informacji, kliknij tutaj: http://www.acronis.pl/my/backup-recovery-online/.

- Aby utworzyć kopię zapasową danych w skarbcu centralnym, rozwiń grupę **Centralne** i kliknij skarbiec.
- Aby utworzyć kopię zapasową danych w skarbcu osobistym, rozwiń grupę **Osobiste** i kliknij skarbiec.

- Aby utworzyć kopię zapasową danych w folderze lokalnym na komputerze, rozwiń grupę **Foldery lokalne** i kliknij żądany folder.
- Aby utworzyć kopię zapasową danych w udziale sieciowym, rozwiń grupę **Foldery sieciowe**, wybierz żądany komputer sieciowy, a następnie kliknij folder udostępniony. Jeśli udział sieciowy wymaga poświadczeń dostępu, program wyświetli odpowiedni monit.

  Uwaga dla użytkowników systemu Linux: *Aby określić udział sieciowy CIFS (Common Internet File System) zamontowany w punkcie montowania takim jak* ***/mnt/share****, należy wybrać ten punkt montowania, a nie sam udział sieciowy.*

- Aby utworzyć kopię zapasową danych na serwerze **FTP** lub **SFTP**, wpisz nazwę i adres serwera w polu **Ścieżka** w następujący sposób:

  ftp://serwer_ftp:numer_portu lub **sftp://serwer_sftp:numer_portu**

  Jeśli nie określisz numeru portu, dla serwera FTP zostanie użyty port 21, a dla SFTP — 22.

  Po wprowadzeniu poświadczeń dostępu zostaną udostępnione foldery na serwerze. Kliknij odpowiedni folder.

  Dostęp do serwera można uzyskać jako użytkownik anonimowy, o ile serwer zezwala na taki dostęp. W tym celu nie trzeba wprowadzać poświadczeń, lecz należy kliknąć opcję **Użyj dostępu anonimowego**.

  Jak wynika z oryginalnej specyfikacji protokołu FTP, poświadczenia wymagane do uzyskania dostępu do serwerów FTP są przesyłane w sieci jako otwarty tekst. Oznacza to, że nazwę użytkownika i hasło można przejąć przy użyciu programu do przechwytywania pakietów.

- Aby utworzyć kopię danych w lokalnie podłączonym urządzeniu taśmowym, rozwiń grupę **Napędy taśmowe**, a następnie kliknij żądane urządzenie.

2. Korzystanie z tabeli archiwum

Aby ułatwić wybór właściwej lokalizacji docelowej, tabela pokazuje nazwy archiwów znajdujących się w każdej wybranej lokalizacji. Podczas przeglądania zawartości lokalizacji inny użytkownik lub sam program mogą dodać, usunąć lub zmodyfikować archiwa według zaplanowanych operacji. Użyj przycisku **Odśwież**, aby odświeżyć listę archiwów.

3. Nadawanie nazwy nowego archiwum

Po wybraniu lokalizacji docelowej archiwum program generuje nazwę nowego archiwum i wyświetla ją w polu **Nazwa**. Standardowo jest to nazwa podobna do Archiwum(1). Wygenerowana nazwa jest unikatowa dla wybranej lokalizacji. Jeśli nazwa wygenerowana automatycznie jest zadawalająca, kliknij **OK**. W przeciwnym razie wprowadź inną unikatową nazwę i kliknij **OK**.

Jeśli nazwa wygenerowana automatycznie wygląda jak *[Typ serwera wirtualizacji] [Nazwa maszyny wirtualnej]*, oznacza to, że nazwa zawiera zmienne. Taka sytuacja może wystąpić, jeśli użytkownik wybrał tworzenie kopii zapasowych danych maszyn wirtualnych. *Typ serwera wirtualizacji* oznacza typ serwera wirtualizacji (ESX, Hyper-V lub inny). *Nazwa maszyny wirtualnej* oznacza nazwę maszyny wirtualnej. Do nazw można dodać sufiksy, ale nigdy nie wolno usuwać zmiennych, ponieważ dane każdej maszyny wirtualnej muszą być kopiowane do oddzielnego archiwum z unikatową nazwą.

Tworzenie kopii zapasowej w istniejącym archiwum

Plan tworzenia kopii zapasowych można skonfigurować tak, aby kopie tworzone były w istniejącym archiwum. W tym celu wybierz archiwum w tabeli lub wpisz nazwę archiwum w polu **Nazwa**. Jeśli archiwum jest chronione hasłem, użytkownik zostanie poproszony o podane hasła w oknie wyskakującym.

Wybierając istniejące archiwum, użytkownik ingeruje w obszar innego planu tworzenia kopii zapasowych, który korzysta z tego samego archiwum. Nie jest to problem, jeśli wykonywanie tego drugiego planu ma zostać przerwane, ale ogólnie należy przestrzegać zasady: „jeden plan tworzenia kopii zapasowych — jedno archiwum”. Działanie niezgodne z tą zasadą nie spowoduje zatrzymania programu, ale nie jest ono ani praktyczne, ani wydajne, z wyjątkiem niektórych szczególnych przypadków.

Dlaczego nie należy tworzyć kopii zapasowych dwóch lub więcej planów w tym samym archiwum

1. Tworzenie kopii zapasowych różnych źródeł w tym samym archiwum utrudnia korzystanie z takiego archiwum. W przypadku odzyskiwania danych liczy się każda sekunda, a w archiwum o takiej zawartości można się zgubić.

   Plany tworzenia kopii zapasowych korzystające z tego samego archiwum powinny uwzględniać w kopii zapasowej identyczne elementy danych (na przykład wolumin C).
2. Stosowanie wielu reguł przechowywania w archiwum sprawia, że w pewien sposób zawartość takiego archiwum trudno jest przewidzieć. Reguły zostaną zastosowane do całego archiwum, dlatego kopie zapasowe należące do jednego planu tworzenia kopii zapasowych mogą być łatwo usunięte razem z kopiami zapasowymi należącymi do innego planu. Może to być szczególnie widoczne w schematach tworzenia kopii zapasowych dziadek-ojciec-syn oraz Wieża Hanoi.

   Zwykle dla każdego złożonego planu tworzenia kopii zapasowych istnieje oddzielne archiwum.

6.2.9 Uproszczone nazewnictwo plików kopii zapasowych

Jeśli zaznaczysz pole wyboru **Plikom kopii zapasowej nadawaj nazwy archiwum...**:

- Nazwa pliku pierwszej (pełnej) kopii zapasowej w archiwum będzie zawierała nazwę archiwum, na przykład: **MojeDane.tib.** Nazwy plików kolejnych (przyrostowych lub różnicowych) kopii zapasowych będą zawierać indeks, na przykład: **MojeDane2.tib**, **MojeDane3.tib** itd.

  Ten prosty schemat nazewnictwa umożliwia utworzenie przenośnego obrazu komputera na nośniku wymiennym lub przeniesienie kopii zapasowych do innej lokalizacji przy użyciu skryptu.
- Przed utworzeniem nowej pełnej kopii zapasowej program usuwa całe archiwum i zakłada nowe.

  Jest to istotne w sytuacji, gdy używane są wymienne dyski twarde USB, a na każdym z nich ma się znajdować jedna pełna kopia zapasowa (s. 233) lub wszystkie kopie zapasowe utworzone w danym tygodniu (s. 233). Może jednak zdarzyć się, że nie zostanie utworzona żadna kopia zapasowa, gdy nie powiedzie się utworzenie pełnej kopii zapasowej na jedynym dysku.

  Ten sposób działania można ograniczyć, dodając do nazwy archiwum zmienną [Date] (s. 235).

Jeśli *nie* zaznaczysz pola wyboru **Plikom kopii zapasowej nadawaj nazwy archiwum...**:

- Każda kopia zapasowa będzie miała unikatową nazwę pliku zawierającą dokładny znacznik czasu oraz typ kopii zapasowej, na przykład: **MojeDane_2010_03_26_17_01_38_960D.tib**. Ten standard nazewnictwa umożliwia używanie szerszego zakresu lokalizacji docelowych kopii zapasowych oraz schematów tworzenia kopii zapasowych.

Ograniczenia

W przypadku używania uproszczonego nazewnictwa plików następujące funkcje są niedostępne:

- Konfigurowanie tworzenia pełnych, przyrostowych i różnicowych kopii zapasowych w jednym planie tworzenia kopii zapasowych. Trzeba utworzyć oddzielne plany tworzenia kopii zapasowych dla każdego z typów kopii.
- Tworzenie kopii zapasowych w skarbcu zarządzanym, na taśmie, w strefie Acronis Secure Zone lub w magazynie Acronis Online Backup Storage

- Konfigurowanie reguł przechowywania
- Konfigurowanie regularnej konwersji kopii zapasowych na maszynę wirtualną
- Używanie liczb na końcu nazwy archiwum

Wskazówka. *Systemy plików FAT16, FAT32 oraz NTFS nie pozwalają na używanie następujących znaków w nazwach plików: ukośnika odwrotnego (\), ukośnika (/), dwukropka (:), gwiazdki (*), pytajnika (?), cudzysłowu ("), znaku mniejszości (<), znaku większości (>), oraz kreski pionowej (|).*

Przykłady użycia

W tej sekcji przedstawiono przykłady użycia uproszczonego nazewnictwa plików.

Przykład 1. Codzienna kopia zapasowa zastępująca starą kopię

Rozważmy następujący scenariusz:

- Chcesz codziennie tworzyć pełną kopię zapasową swojego komputera.
- Chcesz zapisać kopię zapasową lokalnie, w pliku **MójKomputer.tib**.
- Chcesz, aby każda nowa kopia zapasowa zastępowała starą kopię.

W tym scenariuszu musisz utworzyć plan tworzenia kopii zapasowych zawierający codzienny harmonogram. Podczas tworzenia planu tworzenia kopii zapasowych jako nazwę archiwum określ **MójKomputer**, zaznacz pole wyboru **Plikom kopii zapasowej nadawaj nazwy archiwum...**, a następnie wybierz typ kopii zapasowej **Pełna**.

Rezultat. Archiwum składa się z jednego pliku: MójKomputer.tib. Plik jest usuwany przed utworzeniem nowej kopii zapasowej.

Przykład 2. Codzienne pełne kopie zapasowe ze znacznikiem daty

Rozważmy następujący scenariusz:

- Chcesz codziennie tworzyć pełną kopię zapasową swojego komputera.
- Chcesz przenosić stare kopie zapasowe do zdalnej lokalizacji przy użyciu skryptu.

W tym scenariuszu musisz utworzyć plan tworzenia kopii zapasowych zawierający codzienny harmonogram. Podczas tworzenia planu tworzenia kopii zapasowych jako nazwę archiwum określ **MójKomputer-[DATE]**, zaznacz pole wyboru **Plikom kopii zapasowej nadawaj nazwy archiwum...**, a następnie wybierz typ kopii zapasowej **Pełna**.

Rezultat:

- Kopie zapasowe z dnia 1 stycznia 2011 r., 2 stycznia 2011 r. itd. będą zapisywane odpowiednio w plikach MójKomputer-1.1.2011.tib, MójKomputer-1.2.2011.tib itd.
- Twój skrypt może przenosić stare kopie zapasowe na podstawie znacznika daty.

Zobacz także „Zmienna [Date]” (s. 235).

Przykład 3. Kopie zapasowe tworzone co godzinę w ciągu dnia

Rozważmy następujący scenariusz:

- Chcesz codziennie co godzinę tworzyć kopie zapasowe najważniejszych plików serwera.

- Chcesz, aby pierwsza kopia zapasowa była tworzona każdego dnia o północy i była pełna, a kolejne kopie zapasowe w danym dniu były różnicowe, a ich tworzenie było uruchamiane o godzinie 01:00, 02:00 itd.
- Chcesz zachować starsze kopie zapasowe w archiwum.

W tym scenariuszu musisz utworzyć plan tworzenia kopii zapasowych zawierający codzienny harmonogram. Podczas tworzenia planu tworzenia kopii zapasowych jako nazwę archiwum określ **PlikiSerwera([Date])**, zaznacz pole wyboru **Plikom kopii zapasowej nadawaj nazwy archiwum...**, jako typ kopii zapasowej wybierz **Różnicowa**, a następnie zaplanuj tworzenie kopii zapasowych co godzinę od północy.

Rezultat:

- 24 kopie zapasowe z dnia 1 stycznia 2011 r. zostaną zapisane jako Pliki serwera(1.1.2011).tib, PlikiSerwera(1.1.2011)2.tib itd., aż do PlikiSerwera(1.1.2011)24.tib.
- Kolejnego dnia tworzenie kopii zapasowych rozpocznie się od pełnej kopii zapasowej PlikiSerwera(1.2.2011).tib.

Zobacz także „Zmienna [Date]” (s. 235).

Przykład 4. Codzienne pełne kopie zapasowe z codzienną zamianą dysków

Rozważmy następujący scenariusz:

- Chcesz codziennie tworzyć pełne kopie zapasowe komputera w pliku **MójKomputer.tib** na zewnętrznym dysku twardym.
- Masz dwa takie dyski. Do każdego z nich po podłączeniu do komputera jest przypisywana litera dysku **D**.
- Chcesz zamieniać dyski przed każdym utworzeniem kopii zapasowej, tak aby jeden dysk zawierał dzisiejszą kopię zapasową, a drugi wczorajszą kopię zapasową.
- Chcesz, aby każda nowa kopia zapasowa zastępowała kopię znajdującą się na aktualnie podłączonym dysku.

W tym scenariuszu musisz utworzyć plan tworzenia kopii zapasowych zawierający codzienny harmonogram. Podczas tworzenia planu tworzenia kopii zapasowych jako nazwę archiwum określ **MójKomputer**, a jako lokalizację archiwum określ **D:**, zaznacz pole wyboru **Plikom kopii zapasowej nadawaj nazwy archiwum...**, a następnie wybierz typ kopii zapasowej **Pełna**.

Rezultat. Każdy z dysków twardych będzie zawierał jedną pełną kopię zapasową. Gdy jeden z dysków jest podłączony do komputera, drugi z nich możesz przechowywać w innej lokalizacji w celu zapewnienia dodatkowej ochrony danych.

Przykład 5. Codzienne kopie zapasowe z cotygodniową zamianą dysków

Rozważmy następujący scenariusz:

- Chcesz codziennie tworzyć kopie zapasowe komputera: pełną kopię zapasową w każdy poniedziałek, oraz przyrostowe kopie zapasowe od wtorku do niedzieli.
- Chcesz tworzyć kopię zapasową w archiwum **MójKomputer** na zewnętrznym dysku twardym.
- Masz dwa takie dyski. Do każdego z nich po podłączeniu do komputera w systemie operacyjnym jest przypisywana litera dysku **D**.
- Chcesz zamieniać dyski w każdy poniedziałek, tak aby jeden z nich zawierał kopie zapasowe z bieżącego tygodnia (od poniedziałku do niedzieli), a drugi kopie z poprzedniego tygodnia.

W tym scenariuszu musisz utworzyć dwa następujące plany tworzenia kopii zapasowych:

a) Podczas tworzenia pierwszego planu tworzenia kopii zapasowych jako nazwę archiwum określ **MójKomputer**, a jako lokalizację archiwum określ **D:**, zaznacz pole wyboru **Plikom kopii zapasowej nadawaj nazwy archiwum...**, a następnie wybierz typ kopii zapasowej **Pełna** i zaplanuj uruchamianie tworzenia kopii zapasowych co tydzień w poniedziałek.

b) Podczas tworzenia drugiego planu tworzenia kopii zapasowych określ te same ustawienia, ale wybierz typ kopii zapasowej **Przyrostowa** i zaplanuj tworzenie kopii zapasowych co tydzień od wtorku do niedzieli.

Rezultat:

- Przed utworzeniem kopii zapasowej w poniedziałek (według pierwszego planu tworzenia kopii zapasowych) wszystkie kopie zapasowe zostaną usunięte z aktualnie podłączonego dysku.
- Gdy jeden z dysków jest podłączony do komputera, drugi z nich możesz przechowywać w innej lokalizacji w celu zapewnienia dodatkowej ochrony danych.

Przykład 6. Kopie zapasowe w godzinach pracy

Rozważmy następujący scenariusz:

- Chcesz codziennie tworzyć kopie zapasowe najważniejszych plików serwera.
- Chcesz codziennie tworzyć pełną kopię zapasową o godzinie 01:00.
- Chcesz tworzyć różnicowe kopie zapasowe w godzinach pracy, od 8:00 do 17:00 .
- Chcesz do nazwy każdego pliku kopii zapasowej dołączyć datę jej utworzenia.

W tym scenariuszu musisz utworzyć dwa następujące plany tworzenia kopii zapasowych:

a) Podczas tworzenia pierwszego planu tworzenia kopii zapasowych jako nazwę archiwum określ **PlikiSerwera([DATE])**, zaznacz pole wyboru **Plikom kopii zapasowej nadawaj nazwy archiwum...**, jako typ kopii zapasowej wybierz **Pełna**, a następnie zaplanuj tworzenie kopii zapasowych codziennie o godz. 01:00:00 .

b) Podczas tworzenia drugiego planu tworzenia kopii zapasowych określ te same ustawienia, jak dla pierwszego planu, ale wybierz typ kopii zapasowej **Różnicowa** i zaplanuj tworzenie kopii zapasowych w następujący sposób:
   - **Uruchom zadanie**: **Codziennie**
   - **Co**: **1 godz.**
   - **Od**: **08:00:00**
   - **Do**: **17:01:00**

Rezultat:

- Pełna kopia zapasowa z dnia 31 stycznia 2011 r. zostanie zapisana pod nazwą PlikiSerwera(1.31.2011).tib.
- 10 różnicowych kopii zapasowych z dnia 31 stycznia 2011 r. zostanie zapisanych pod nazwami PlikiSerwera(1.31.2011)2.tib, PlikiSerwera(1.31.2011)3.tib itd., aż do PlikiSerwera(1.31.2011)11.tib.
- Kolejnego dnia, 1 lutego 2011 r., tworzenie kopii zapasowych rozpocznie się od pełnej kopii zapasowej PlikiSerwera(2.1.2011).tib. Różnicowe kopie zapasowe będą się rozpoczynały od pliku PlikiSerwera(2.1.2011)2.tib.

Zobacz także „Zmienna [Date]” (s. 235).

Zmienna [DATE]

Jeśli w nazwie archiwum określisz zmienną **[DATE]**, do nazwy pliku każdej kopii zapasowej program dołączy datę utworzenia tej kopii.

W przypadku użycia tej zmiennej pierwsza kopia zapasowa utworzona danego dnia będzie pełną kopią zapasową. Przed utworzeniem kolejnej pełnej kopii zapasowej program usunie wszystkie kopie zapasowe utworzone wcześniej tego samego dnia. Kopie zapasowe utworzone w poprzednich dniach zostaną zachowane. Oznacza to, że możesz zapisać kilka pełnych kopii zapasowych wraz z kopiami przyrostowymi lub bez nich, ale nie więcej niż jedną pełną kopię zapasową dziennie. Kopie zapasowe możesz sortować według daty, kopiować, przenosić, usuwać ręcznie lub przy użyciu skryptu.

Format daty to: *m.d.rrrr*. Na przykład 1.31.2011 oznacza 31 stycznia 2011 roku. (Nie występują zera wiodące).

Możesz umieścić tę zmienną w dowolnym miejscu w nazwie archiwum. W tej zmiennej możesz użyć zarówno wielkich, jak i małych liter.

Przykłady

Przykład 1. Przyjmijmy, że tworzysz przyrostowe kopie zapasowe dwa razy dziennie (o północy i w południe) przez dwa dni, rozpoczynając od 31 stycznia 2011 r. Jeśli nazwa archiwum ma postać **MojeArchiwum-[DATE]-**, lista plików kopii zapasowych po zakończeniu drugiego dnia będzie następująca:

MojeArchiwum-1.31.2011-.tib (pełna, utworzona 31 stycznia o północy)
MojeArchiwum-1.31.2011-2.tib (przyrostowa, utworzona 31 stycznia w południe)
MojeArchiwum-2.1.2011-.tib (pełna, utworzona 1 lutego o północy)
MojeArchiwum-2.1.2011-2.tib (przyrostowa, utworzona 1 lutego w południe)

Przykład 2. Przyjmijmy, że tworzysz pełne kopie zapasowe według tego samego schematu, oraz używając takiej samej nazwy archiwum, jak w poprzednim przykładzie. Lista plików kopii zapasowych po zakończeniu drugiego dnia będzie wówczas następująca:

MojeArchiwum-1.31.2011-.tib (pełna, utworzona 31 stycznia w południe)
MojeArchiwum-2.1.2011-.tib (pełna, utworzona 1 lutego w południe)

Wynika to z zastąpienia pełnych kopii zapasowych utworzonych o północy przez nowe pełne kopie zapasowe utworzone w południe.

Podział kopii zapasowych i uproszczone nazewnictwo plików

Podczas podziału kopii zapasowej (s. 125) zgodnie z ustawieniami takie samo indeksowanie służy do nadawania nazw poszczególnym częściom kopii zapasowej. Do nazwy pliku kolejnej kopii zapasowej program przydzieli kolejny wolny indeks.

Przyjmijmy na przykład, że pierwsza kopia zapasowa archiwum **MojeDane** została podzielona na dwie części. Nazwy plików tej kopii zapasowej będą następujące: **MojeDane1.tib** i **MojeDane2.tib**. Kolejna kopia zapasowa (przyjmijmy, że nie jest dzielona) będzie miała nazwę **MojeDane3.tib**.

6.2.10 Poświadczenia dostępu do lokalizacji archiwum

Określ poświadczenia wymagane w celu dostępu do lokalizacji przechowywania archiwum kopii zapasowych. Użytkownik, którego nazwa została określona, będzie uważany za właściciela archiwum.

Aby określić poświadczenia

1. Wybierz jedną z następujących opcji:

- **Użyj poświadczeń planu**

  Program uzyska dostęp do danych źródłowych przy użyciu poświadczeń konta planu tworzenia kopii zapasowych określonych w sekcji Ogólne.

- **Użyj następujących poświadczeń**

  Program uzyska dostęp do danych źródłowych przy użyciu określonych poświadczeń. Użyj tej opcji, jeśli konto planu nie posiada uprawnień dostępu do lokalizacji. Może być konieczne podanie specjalnych poświadczeń udziału sieciowego lub skarbca węzła magazynowania.

  Określ:

  - **Nazwa użytkownika**. Wprowadzając nazwę konta użytkownika usługi Active Directory, należy określić również nazwę domeny (DOMENA\Nazwa_użytkownika lub Nazwa_użytkownika@domena).
  - **Hasło**. Hasło dla konta.

2. Kliknij **OK**.

Ostrzeżenie: *Jak wynika z oryginalnej specyfikacji protokołu FTP, poświadczenia wymagane do uzyskania dostępu do serwerów FTP są przesyłane w sieci jako otwarty tekst. Oznacza to, że nazwę użytkownika i hasło można przejąć przy użyciu programu do przechwytywania pakietów.*

6.2.11 Schematy tworzenia kopii zapasowych

Wybierz jeden z dostępnych schematów tworzenia kopii zapasowych:

- **Utwórz kopię zapasową** — aby utworzyć zadanie tworzenia kopii zapasowej przeznaczone do ręcznego uruchamiania oraz uruchomić to zadanie natychmiast po utworzeniu.
- **Utwórz kopię zapasową później** — aby utworzyć zadanie tworzenia kopii zapasowej przeznaczone do ręcznego uruchamiania LUB zaplanować jednorazowe wykonanie zadania w przyszłości.
- **Prosty** — aby zaplanować czas i częstotliwość tworzenia kopii zapasowych danych oraz określić reguły przechowywania.
- **Dziadek-ojciec-syn** — aby użyć schematu tworzenia kopii zapasowych Dziadek-ojciec-syn. Schemat ten umożliwia tworzenie kopii zapasowej danych najwyżej raz dziennie. Użytkownik wyznacza dni wykonywania dziennej kopii zapasowej i spośród tych dni wybiera dzień tworzenia kopii tygodniowej/miesięcznej. Następnie ustawia okresy przechowywania kopii zapasowych dziennych (zwanych „synami”), tygodniowych (zwanych „ojcami”) i miesięcznych (zwanych „dziadkami”). Nieaktualne kopie zapasowe będą usuwane automatycznie.
- **Wieża Hanoi** — aby użyć schematu tworzenia kopii zapasowych Wieża Hanoi, w którym użytkownik planuje czas i częstotliwość tworzenia kopii zapasowych (sesje) oraz wybiera liczbę poziomów kopii (maksymalnie 16). W tym schemacie kopie zapasowe można wykonywać częściej niż raz dziennie. Konfigurując schemat i wybierając poziomy tworzenia kopii zapasowych, automatycznie uzyskuje się okres wycofywania, czyli gwarantowaną liczbę sesji, o którą można się cofnąć w dowolnym momencie. Mechanizm automatycznego czyszczenia umożliwia zachowanie wymaganego okresu wycofywania dzięki usuwaniu nieaktualnych kopii zapasowych i zachowywaniu najnowszych kopii na każdym poziomie.
- **Niestandardowy** — aby utworzyć schemat tworzenia kopii zapasowych, w którym użytkownik może dowolnie konfigurować strategię tworzenia kopii w sposób najlepiej odpowiadający potrzebom przedsiębiorstwa. Można zdefiniować wiele harmonogramów dla różnych typów kopii zapasowych, dodać warunki i określić reguły przechowywania.
- **Pierwotna kopia zapasowa w magazynie** — aby zapisać lokalnie pełną kopię zapasową, której ostatecznym miejscem docelowym jest magazyn Acronis Online Backup Storage.

Schemat „Utwórz kopię zapasową”

W schemacie **Utwórz kopię zapasową** kopia zapasowa zostanie wykonana niezwłocznie po kliknięciu przycisku **OK** u dołu strony.

W polu **Typ kopii zapasowej** wybierz, czy utworzyć pełną, przyrostową lub różnicową kopię zapasową (s. 36).

Schemat „Utwórz kopię zapasową później”

W schemacie „Utwórz kopię zapasową później” kopia zapasowa zostanie utworzona tylko raz — o godzinie i w dniu określonym przez użytkownika.

Określ właściwe ustawienia w następujący sposób

Typ kopii zapasowej	Wybierz typ kopii zapasowej: pełna, przyrostowa lub różnicowa. Jeśli archiwum nie zawiera pełnej kopii zapasowej, zostanie ona utworzona niezależnie od dokonanego wyboru.
Data i godzina	Określ początek tworzenia kopii zapasowej.
Zadanie zostanie uruchomione ręcznie	Zaznacz to pole wyboru, jeśli nie chcesz dołączyć zadania do harmonogramu i zamierzasz uruchomić je ręcznie później.

Schemat prosty

W schemacie prostym wystarczy zaplanować czas i częstotliwość tworzenia kopii zapasowej danych oraz zdefiniować regułę przechowywania. Za pierwszym razem zostanie utworzona pełna kopia zapasowa. Następne kopie zapasowe będą przyrostowe.

Aby skonfigurować prosty schemat tworzenia kopii zapasowych, określ właściwe ustawienia w następujący sposób:

Kopia zapasowa	Skonfiguruj harmonogram tworzenia kopii zapasowych — czas i częstotliwość wykonywania kopii zapasowej danych. Aby dowiedzieć się więcej na temat konfigurowania harmonogramu, zobacz sekcję Tworzenie harmonogramu (s. 185).
Reguła przechowywania	W schemacie prostym dostępna jest tylko jedna reguła przechowywania (s. 45). Zdefiniuj okres przechowywania kopii zapasowych.

Schemat Dziadek-ojciec-syn

W skrócie

- Dzienne przyrostowe, tygodniowe różnicowe i miesięczne pełne kopie zapasowe
- Wybór dnia tworzenia tygodniowych i miesięcznych kopii zapasowych
- Wybór okresów przechowywania kopii zapasowych każdego typu

Opis

Załóżmy, że chcemy skonfigurować plan tworzenia kopii zapasowych, w ramach którego regularnie wykonywane będą dzienne (D), tygodniowe (T) i miesięczne (M) kopie zapasowe. Oto najprostszy sposób: poniższa tabela przedstawia przykładowy dwumiesięczny okres takiego planu.

	Pn	Wt	Śr	Cz	Pt	Sb	Nd
1 sty–7 sty	D	D	D	D	T	-	-

8 sty–14 sty	D	D	D	D	T	-	-
15 sty–21 sty	D	D	D	D	T	-	-
22 sty–28 sty	D	D	D	D	M	-	-
29 sty–4 lut	D	D	D	D	T	-	-
5 lut–11 lut	D	D	D	D	T	-	-
12 lut–18 lut	D	D	D	D	T	-	-
19 lut–25 lut	D	D	D	D	M	-	-
26 lut–4 mar	D	D	D	D	T	-	-

Dzienne kopie zapasowe są wykonywane każdego dnia z wyjątkiem piątku, który został wyznaczony na tworzenie tygodniowych i miesięcznych kopii zapasowych. Miesięczne kopie zapasowe są wykonywane co czwarty piątek, natomiast tygodniowe kopie zapasowe we wszystkie pozostałe piątki.

- Miesięczne kopie zapasowe („dziadek”) to kopie pełne.
- Tygodniowe kopie zapasowe („ojciec”) to kopie różnicowe.
- Dzienne kopie zapasowe („syn”) to kopie przyrostowe.

Parametry

W schemacie Dziadek-ojciec-syn (GFS) można skonfigurować poniższe parametry.

Rozpocznij tworzenie kopii zapasowej o:	Określa godzinę rozpoczęcia tworzenia kopii zapasowej. Wartość domyślna to 12:00.
Utwórz kopię zapasową dnia:	Określa dni wykonywania kopii zapasowej. Wartość domyślna to dni robocze.
Tygodniowa/miesięczna:	Określa dzień spośród dni wybranych w polu **Utwórz kopię zapasową** dnia, który jest zarezerwowany na tworzenie tygodniowych i miesięcznych kopii zapasowych. Miesięczna kopia zapasowa będzie wykonywana co czwarty taki dzień. Wartość domyślna to piątek.

Zachowuj kopie zapasowe:	Określa czas przechowywania kopii zapasowych w archiwum. Czas przechowywania można określić w godzinach, dniach, tygodniach, miesiącach lub latach. Miesięczne kopie zapasowe można przechowywać bez ograniczeń czasowych, wybierając opcję **Zachowaj w nieskończoność**. Poniżej znajdują się wartości domyślne dla każdego typu kopii zapasowej. Dzienna: 7 dni (zalecane minimum) Tygodniowa: 4 tygodnie Miesięczna: w nieskończoność Okres przechowywania tygodniowych kopii zapasowych musi być dłuższy niż okres przechowywania kopii dziennych. Okres przechowywania miesięcznych kopii zapasowych musi być dłuższy niż okres przechowywania kopii tygodniowych. Zaleca się przynajmniej jednotygodniowy okres przechowywania dziennych kopii zapasowych.

Niezależnie od ustawień kopia zapasowa nie zostanie usunięta, dopóki nie zostaną usunięte jej wszystkie kopie zależne. Dlatego tygodniowe lub miesięczne kopie zapasowe mogą pozostawać w archiwum przez kilka dni po spodziewanej dacie utraty ważności.

Jeśli harmonogram rozpoczyna się od dziennej lub tygodniowej kopii zapasowej, zamiast niej zostanie utworzona pełna kopia zapasowa.

Przykłady

Każdy dzień ostatniego tygodnia, każdy tydzień ostatniego miesiąca

Rozważmy schemat tworzenia kopii zapasowych Dziadek-ojciec-syn, który może okazać się przydatny w wielu sytuacjach.

- Kopie zapasowe plików tworzone codziennie, w tym w sobotę i niedzielę
- Zapewnienie możliwości odzyskania plików do stanu na dowolny z ostatnich siedmiu dni
- Zapewnienie dostępu do tygodniowych kopii zapasowych ostatniego miesiąca
- Zachowywanie miesięcznych kopii zapasowych w nieskończoność

Parametry schematu tworzenia kopii zapasowych można skonfigurować w następujący sposób:

- Rozpocznij tworzenie kopii zapasowej o: **23.00**
- Utwórz kopię zapasową dnia: **Wszystkie dni**
- Tygodniowa/miesięczna: **Sobota** (przykładowo)
- Zachowuj kopie zapasowe:
  - Codzienna: **1 tydzień**
  - Tygodniowa: **1 miesiąc**
  - Miesięczna: **w nieskończoność**

W wyniku tych ustawień zostanie utworzone archiwum codziennych, tygodniowych i miesięcznych kopii zapasowych. Codzienne kopie zapasowe będą dostępne przez siedem dni od momentu ich

utworzenia. Codzienna kopia zapasowa utworzona np. w niedzielę 1 stycznia będzie dostępna do następnej niedzieli 8 stycznia. Pierwsza tygodniowa kopia zapasowa utworzona w sobotę 7 stycznia będzie przechowywana w systemie do 7 lutego. Miesięczne kopie zapasowe nie zostaną nigdy usunięte.

Ograniczone miejsce przechowywania

Aby nie przeznaczać dużej ilości miejsca na ogromne archiwum, schemat Dziadek-ojciec-syn (GFS) można skonfigurować tak, aby krócej przechowywać kopie zapasowe, a jednocześnie zapewnić odzyskanie danych w razie ich przypadkowej utraty.

Przyjmijmy następujące założenia:

- kopie zapasowe mają być wykonywane na koniec każdego dnia roboczego;
- musi istnieć możliwość odzyskania przypadkowo usuniętego lub nieumyślnie zmodyfikowanego pliku, jeśli zostało to wykryte relatywnie szybko;
- dostęp do tygodniowej kopii zapasowej musi być zapewniony przez 10 dni od momentu jej utworzenia;
- miesięczne kopie zapasowe muszą być zachowywane przez pół roku.

Parametry schematu tworzenia kopii zapasowych można skonfigurować w następujący sposób:

- Rozpocznij tworzenie kopii zapasowej o: **18.00**
- Utwórz kopię zapasową dnia: **Dni robocze**
- Tygodniowa/miesięczna: **piątek**
- Zachowuj kopie zapasowe:
  - Codzienna: **1 tydzień**
  - Tygodniowa: **10 dni**
  - Miesięczna: **6 miesięcy**

W tym schemacie użytkownik ma tydzień na odzyskanie poprzedniej wersji uszkodzonego pliku z codziennej kopii zapasowej, a także 10-dniowy dostęp do tygodniowych kopii zapasowych. Każda miesięczna pełna kopia zapasowa będzie dostępna przez sześć miesięcy od daty jej utworzenia.

Harmonogram prac

Załóżmy, że jesteś konsultantem finansowym i pracujesz w firmie na pół etatu we wtorki i czwartki. W te dni dokonujesz zmian w dokumentach i sprawozdaniach finansowych, aktualizujesz arkusze kalkulacyjne itp. na komputerze przenośnym. Aby utworzyć kopie zapasowe tych danych możesz:

- Śledzić zmiany w sprawozdaniach finansowych, arkuszach kalkulacyjnych itp. we wtorki i czwartki (codzienna przyrostowa kopia zapasowa).
- Sporządzać tygodniowe podsumowania zmian plików w porównaniu z ostatnim miesiącem (tygodniowa różnicowa kopia zapasowa w każdy piątek).
- Raz na miesiąc robić pełną kopię zapasową plików.

Ponadto załóżmy, że chcesz zachować wszystkie kopie zapasowe — w tym dzienne — przez co najmniej sześć miesięcy.

Do tych celów odpowiedni jest następujący schemat „dziadek-ojciec-syn” (GFS):

- Rozpocznij tworzenie kopii zapasowej o: **23:30**
- Utwórz kopię zapasową dnia: **wtorek, czwartek, piątek**
- Tygodniowa/miesięczna: **piątek**

- Zachowuj kopie zapasowe:
  - Codzienna: **6 miesięcy**
  - Tygodniowa: **6 miesięcy**
  - Miesięczna: **5 lat**

W tym przykładzie dzienne przyrostowe kopie zapasowe będą wykonywane we wtorki i czwartki, natomiast kopie tygodniowe i miesięczne w piątki. Uwaga: aby wybrać **piątek** w polu **Tygodniowa/miesięczna**, trzeba najpierw zaznaczyć ten dzień w polu **Utwórz kopię zapasową dnia**.

Takie archiwum umożliwi porównanie dokumentów finansowych na pierwszy i ostatni dzień pracy oraz utworzenie pięcioletniej historii wszystkich dokumentów itp.

Bez dziennych kopii zapasowych

Przeanalizujmy bardziej egzotyczny schemat „dziadek-ojciec-syn” (GFS):

- Rozpocznij tworzenie kopii zapasowej o: **12.00 w południe**
- Utwórz kopię zapasową dnia: **piątek**
- Tygodniowa/miesięczna: **piątek**
- Zachowuj kopie zapasowe:
  - Codzienna: **1 tydzień**
  - Tygodniowa: **1 miesiąc**
  - Miesięczna: **w nieskończoność**

Zatem kopie zapasowe będą wykonywane w piątki. W ten sposób piątek będzie jedynym dniem tworzenia tygodniowych i miesięcznych kopii zapasowych, bez wyboru dnia dla kopii dziennych. Tak więc powstałe archiwum „dziadek-ojciec” będzie składać się tylko z tygodniowych kopii różnicowych i miesięcznych pełnych kopii zapasowych.

Chociaż można użyć schematu „dziadek-ojciec-syn” do utworzenia takiego archiwum, w tej sytuacji schemat niestandardowy zapewni większą elastyczność.

Schemat Wieża Hanoi

W skrócie

- Maksymalnie 16 poziomów pełnych, różnicowych i przyrostowych kopii zapasowych.
- Kopie zapasowe kolejnego poziomu występują dwa razy rzadziej niż kopie zapasowe poprzedniego poziomu.
- Jednocześnie jest przechowywana tylko jedna kopia zapasowa każdego poziomu.
- Większe zagęszczenie nowszych kopii zapasowych.

Parametry

Można skonfigurować następujące parametry schematu Wieża Hanoi:

Harmonogram	Skonfiguruj harmonogram codzienny (s. 186), tygodniowy (s. 188) lub miesięczny (s. 190). Konfiguracja parametrów harmonogramu umożliwia tworzenie harmonogramów prostych (przykład prostego harmonogramu codziennego: zadanie tworzenia kopii zapasowej uruchamiane codziennie o 10.00) oraz harmonogramów bardziej złożonych (przykład złożonego harmonogramu codziennego: zadanie uruchamiane co trzy dni, począwszy od 15 stycznia. Zadanie będzie powtarzane w określone dni co dwie godziny od 10.00 do 22.00). W ten sposób harmonogram złożony określa sesje, podczas których schemat będzie

	stosowany. W omówieniu znajdującym się poniżej pojęcie „dni” można zastąpić terminem „sesje zaplanowane”.
Liczba poziomów	Wybierz od 2 do 16 poziomów tworzenia kopii zapasowych. Zobacz szczegółowy przykład poniżej.
Okres wycofywania	Gwarantowana liczba sesji, podczas których można przywrócić kopie z archiwum w dowolnym momencie. Obliczana jest automatycznie na podstawie parametrów harmonogramu i liczby poziomów określonych przez użytkownika. Zobacz szczegółowy przykład poniżej.

Przykład

Parametry **harmonogramu** są następujące

- Powtarzaj co: 1 dzień
- Częstotliwość: Raz o 18.00

Liczba poziomów: 4

Pierwsze 14 dni (lub 14 sesji) harmonogramu tego schematu będą wyglądały jak poniżej. Liczby zacienione oznaczają poziomy tworzenia kopii zapasowych.

1	2	3	4	5	6	7	8	9	10	11	12	13	14
4	1	2	1	3	1	2	1	4	1	2	1	3	1

Kopie zapasowe różnych poziomów są różnego typu:

- kopie zapasowe *ostatniego poziomu* (w tym przypadku poziom 4) to kopie pełne;
- kopie zapasowe *średniego poziomu* (2, 3) to kopie różnicowe;
- kopie zapasowe *pierwszego poziomu* (1) to kopie przyrostowe.

Zastosowanie mechanizmu czyszczenia umożliwia zachowanie tylko najnowszych kopii zapasowych każdego poziomu. W dniu 8 — dzień przed utworzeniem nowej pełnej kopii zapasowej — archiwum będzie wyglądało następująco.

1	2	3	4	5	6	7	8
4	1	2	1	3	1	2	1

Ten schemat zapewnia wydajne przechowywanie danych: więcej kopii zapasowych jest skumulowanych w okolicach aktualnego czasu. Mając cztery kopie zapasowe, można odzyskać dane zapisane dziś, wczoraj, w połowie tygodnia lub tydzień temu.

Okres wycofywania

Liczba dni, podczas których można powracać do kopii zapasowych znajdujących się w archiwum, jest inna w różne dni. Minimalną zagwarantowaną liczbę dni nazywa się okresem wycofywania.

Tabela poniżej pokazuje okresy tworzenia i wycofywania kopii zapasowych dla schematów z różnymi poziomami.

Liczba poziomów	Pełna kopia zapasowa co	W zależności od dnia można powrócić	Okres wycofywania
2	2 dni	od 1 do 2 dni	1 dzień

3	4 dni	od 2 do 5 dni	2 dni
4	8 dni	od 4 do 11 dni	4 dni
5	16 dni	od 8 do 23 dni	8 dni
6	32 dni	od 16 do 47 dni	16 dni

Dodanie poziomu powoduje podwojenie okresów tworzenia pełnej kopii zapasowej oraz wycofywania.

Wróćmy do poprzedniego przykładu, aby zobaczyć, dlaczego liczba dni odzyskiwania się zmienia.

Oto kopie zapasowe w dniu 12 (liczby w kolorze szarym oznaczają usunięte kopie zapasowe).

1	2	3	4	5	6	7	8	9	10	11	12
4	1	2	1	3	1	2	1	4	1	2	1

Nowa różnicowa kopia zapasowa na poziomie 3 jeszcze nie została utworzona, zatem kopia dnia piątego jest nadal przechowywana. Jest ona zależna od pełnej kopii zapasowej dnia pierwszego, dlatego jest również dostępna. Dzięki temu możemy cofnąć się aż o 11 dni, co jest najlepszym scenariuszem w tym przypadku.

Jednak w następnym dniu zostanie utworzona nowa różnicowa kopia zapasowa trzeciego poziomu, a stara pełna kopia zapasowa zostanie usunięta.

1	2	3	4	5	6	7	8	9	10	11	12	13
4	1	2	1	3	1	2	1	4	1	2	1	3

To daje zaledwie czterodniowy okres na odzyskiwanie danych, co okazuje się być najgorszym scenariuszem w tym przypadku.

W dniu 14 ten okres wynosi pięć dni. W kolejne dni wydłuża się, zanim ponownie zacznie się skracać itd.

1	2	3	4	5	6	7	8	9	10	11	12	13	14
4	1	2	1	3	1	2	1	4	1	2	1	3	1

Parametr Okres wycofywania pokazuje zagwarantowaną liczbę dni na odzyskiwanie danych nawet w najgorszym przypadku. Przy schemacie z czterema poziomami wynosi on cztery dni.

Niestandardowy schemat tworzenia kopii zapasowych

W skrócie

- Niestandardowy harmonogram i warunki tworzenia kopii zapasowych każdego typu
- Niestandardowy harmonogram i reguły przechowywania

Parametry

Parametr	Znaczenie
Pełna kopia zapasowa	Określa harmonogram i warunki wykonywania pełnej kopii zapasowej. Można na przykład tak skonfigurować tworzenie pełnej kopii zapasowej, aby była wykonywana w każdą niedzielę o 1:00 po wylogowaniu się wszystkich użytkowników.
Przyrostowa	Określa harmonogram i warunki wykonywania przyrostowej kopii zapasowej. Jeśli w momencie uruchomienia zadania archiwum nie zawiera pełnych kopii zapasowych, zamiast kopii przyrostowej tworzona jest pełna kopia zapasowa.

Różnicowa	Określa harmonogram i warunki wykonywania różnicowej kopii zapasowej. Jeśli w momencie uruchomienia zadania archiwum nie zawiera pełnych kopii zapasowych, zamiast kopii różnicowej tworzona jest pełna kopia zapasowa.
Czyszczenie archiwum	Określa sposób usuwania starych kopii zapasowych. Dwie dostępne możliwości to regularne stosowanie reguł przechowywania (s. 45) i czyszczenie archiwum po tym, gdy w docelowej lokalizacji zabraknie miejsca. W domyślnej konfiguracji reguły przechowywania nie są określone. Oznacza to, że starsze kopie zapasowe nie zostaną automatycznie usunięte. **Używanie reguł przechowywania** Określ reguły przechowywania i warunki ich stosowania. To ustawienie jest zalecane dla takich lokalizacji kopii zapasowych, jak foldery udostępnione lub skarbce centralne. **Gdy w trakcie tworzenia kopii zapasowej zabraknie miejsca.** Archiwum zostanie wyczyszczone tylko wtedy, gdy podczas tworzenia kopii zapasowej zabraknie miejsca na utworzenie nowej kopii. W takiej sytuacji program wykona następujące czynności: ▪ Usunięcie najstarszej pełnej kopii zapasowej razem ze wszystkimi zależnymi kopiami przyrostowymi/różnicowymi. ▪ Gdy dostępna jest tylko jedna pełna kopia zapasowa, ale trwa wykonywanie pełnej kopii zapasowej, istniejąca pełna kopia zapasowa zostanie usunięta razem ze wszystkimi zależnymi kopiami przyrostowymi/różnicowymi. ▪ Gdy dostępna jest tylko jedna pełna kopia zapasowa, ale trwa wykonywanie przyrostowej lub różnicowej kopii zapasowej, zostanie wyświetlony błąd o braku dostępnego miejsca. Ustawienie to jest zalecane podczas wykonywania kopii zapasowych na pamięć USB lub do strefy Acronis Secure Zone. Ustawienie to nie dotyczy skarbców zarządzanych. Ustawienie to umożliwia usunięcie ostatniej kopii zapasowej w archiwum w sytuacji, w której urządzenie pamięci masowej nie może pomieścić więcej niż jednej kopii. Jednak jeśli program z jakiegoś powodu nie może utworzyć nowej kopii zapasowej, może dojść do sytuacji, w której nie będzie dostępna żadna kopia zapasowa.
Zastosuj reguły (tylko po skonfigurowaniu reguł przechowywania)	Określa, kiedy należy zastosować reguły przechowywania (s. 45). Procedurę czyszczenia można na przykład skonfigurować tak, aby była uruchamiana po każdym wykonaniu kopii zapasowej, a także według harmonogramu. Ta opcja jest dostępna tylko pod warunkiem, że w sekcji **Reguły przechowywania** została skonfigurowana przynajmniej jedna reguła przechowywania.
Harmonogram czyszczenia (tylko po wybraniu opcji **Według harmonogramu**)	Określa harmonogram procedury czyszczenia archiwum. Rozpoczęcie czyszczenia można na przykład zaplanować na ostatni dzień każdego miesiąca. Ta opcja jest dostępna tylko w przypadku wybrania parametru **Według harmonogramu** w sekcji **Zastosuj reguły**.

Przykłady

Tygodniowa pełna kopia zapasowa

Poniższy schemat umożliwia tworzenie pełnej kopii zapasowej w każdy piątek wieczorem.

Pełna kopia zapasowa: **Harmonogram: Co tydzień**, w każdy **piątek** o **22.00..**

W tym przykładzie pola wszystkich parametrów z wyjątkiem **Harmonogram** w **Pełna kopia zapasowa** pozostają puste. Wszystkie kopie zapasowe w archiwum są przechowywane w nieskończoność (bez czyszczenia archiwów).

Pełna i przyrostowa kopia zapasowa plus czyszczenie

W następującym schemacie archiwum zawiera tygodniowe pełne i codzienne przyrostowe kopie zapasowe. Oprócz tego wymagamy również, aby program wykonał pełną kopię zapasową tylko po wylogowaniu wszystkich użytkowników.

Pełna kopia zapasowa: Harmonogram: Co tydzień, w każdy **Piątek** o **22.00.**

Pełna kopia zapasowa: Warunki: Użytkownik wylogowany.

Przyrostowa kopia zapasowa: Harmonogram: Co tydzień, w każdy dzień roboczy o **21.00.**

Dodatkowo ustalamy usuwanie z archiwum kopii zapasowych starszych niż jeden rok oraz wykonywanie procedury czyszczenia po utworzeniu nowej kopii zapasowej.

Reguły przechowywania: Usuwaj kopie zapasowe starsze niż **12 miesięcy.**

Zastosuj reguły: Po wykonaniu kopii zapasowej.

Domyślnie jednoroczna pełna kopia zapasowa nie zostanie usunięta, dopóki wszystkie zależne od niej przyrostowe kopie zapasowe nie zostaną również usunięte. Więcej informacji znajduje się w sekcji Reguły przechowywania (s. 45).

Miesięczne pełne, tygodniowe różnicowe i dzienne przyrostowe kopie zapasowe plus czyszczenie.

Ten przykład pokazuje zastosowanie wszystkich dostępnych opcji w schemacie niestandardowym.

Załóżmy, że chcemy stworzyć schemat, w ramach którego będą wykonywane miesięczne pełne kopie zapasowe, tygodniowe różnicowe kopie zapasowe i dzienne przyrostowe kopie zapasowe. Wówczas harmonogram tworzenia kopii zapasowych będzie wyglądał jak poniżej.

Pełna kopia zapasowa: Harmonogram: Co miesiąc, w każdą **ostatnią niedzielę** miesiąca o **21.00.**

Przyrostowa kopia zapasowa: Harmonogram: Co tydzień, w każdy **dzień roboczy** o **19.00.**

Różnicowa kopia zapasowa: Harmonogram: Co tydzień, w każdą **sobotę** o **20.00.**

Oprócz tego chcemy dodać warunki, które muszą zostać spełnione, aby uruchomić zadanie tworzenia kopii zapasowej. Określa się je w polach **Warunki** dla każdego typu kopii zapasowej.

Pełna kopia zapasowa: **Warunki**: **Lokalizacja jest dostępna.**

Przyrostowa kopia zapasowa: **Warunki**: **Użytkownik wylogowany.**

Różnicowa kopia zapasowa: **Warunki**: **Użytkownik jest bezczynny.**

Przy takich ustawieniach wykonanie pełnej kopii zapasowej — pierwotnie zaplanowanej na 21.00 — może faktycznie rozpocząć się później: gdy tylko będzie dostępna lokalizacja kopii zapasowej. Podobnie zadania tworzenia przyrostowych i różnicowych kopii zapasowych zostaną uruchomione dopiero, kiedy wszyscy użytkownicy odpowiednio wylogują się i będą bezczynni.

Na koniec tworzymy reguły przechowywania kopii w archiwum: zachowajmy tylko te kopie zapasowe, które nie są starsze niż sześć miesięcy i zezwólmy na wykonanie czyszczenia po każdym zadaniu tworzenia kopii zapasowej oraz również ostatniego dnia każdego miesiąca.

Reguły przechowywania: Usuwaj kopie zapasowe starsze niż **6 miesięcy.**

Zastosuj reguły: **After backing up (Po utworzeniu kopii zapasowej)**, **Według harmonogramu.**

Harmonogram czyszczenia: **Co miesiąc**, **Ostatni dzień**, **Wszystkie miesiące**, o **22.00.**

Domyślnie program nie usuwa kopii zapasowej, dopóki istnieją zależne kopie zapasowe, które muszą zostać zachowane. Jeżeli na przykład pełna kopia zapasowa przeznaczona do usunięcia posiada zależne kopie przyrostowe lub różnicowe, usunięcie zostanie odłożone do momentu, kiedy będzie można usunąć również kopie zależne.

Więcej informacji znajduje się w części Reguły przechowywania (s. 45).

Zadania wynikowe

W każdym schemacie niestandardowym program zawsze generuje trzy zadania tworzenia kopii zapasowych oraz — jeśli określono reguły przechowywania — zadanie czyszczenia. Każde zadanie widnieje na liście zadań albo jako **Zaplanowane** (jeśli został skonfigurowany harmonogram), albo jako **Ręczne** (jeśli harmonogram nie został skonfigurowany).

Każde zadanie tworzenia kopii zapasowej lub zadanie czyszczenia można w dowolnym momencie uruchomić ręcznie — niezależnie od tego, czy znajduje się w harmonogramie.

W pierwszym z wcześniejszych przykładów skonfigurowany harmonogram przewidywał tworzenie tylko pełnych kopii zapasowych. Jednak schemat mimo to spowoduje powstanie trzech zadań, umożliwiając ręczne uruchomienie zadania tworzenia kopii zapasowej dowolnego typu:

- Tworzenie pełnej kopii zapasowej, uruchamiane w każdy piątek o 22:00
- Tworzenie przyrostowej kopii zapasowej, uruchamiane ręcznie
- Tworzenie różnicowej kopii zapasowej, uruchamiane ręcznie

Dowolne z tych zadań tworzenia kopii zapasowych można uruchomić, wybierając je z listy zadań w sekcji **Plany i zadania tworzenia kopii zapasowych** w lewym panelu.

Jeśli w schemacie tworzenia kopii zapasowych określono również reguły przechowywania, schemat spowoduje powstanie czterech zadań: trzech zadań tworzenia kopii zapasowych oraz jednego zadania czyszczenia.

6.2.12 Sprawdzanie poprawności archiwum

Należy skonfigurować zadanie sprawdzania poprawności, aby sprawdzić możliwość odzyskania danych z kopii zapasowych. Jeśli proces sprawdzania poprawności kopii zapasowej nie zakończy się pomyślnie, zadanie sprawdzania poprawności zakończy się niepowodzeniem, a plan tworzenia kopii zapasowych otrzyma status Błąd.

Aby skonfigurować sprawdzanie poprawności, określ następujące parametry

1. **Czas sprawdzania poprawności** — wybierz czas wykonywania zadania sprawdzania poprawności. Sprawdzanie poprawności to operacja intensywnie korzystająca z zasobów i zaleca się **zaplanowanie** sprawdzania poprawności na komputerze zarządzanym poza okresem największego ruchu. Jednak jeśli sprawdzanie poprawności stanowi zasadniczą część strategii ochrony danych i użytkownik chce niezwłocznie wiedzieć, czy dane kopii zapasowej są

uszkodzone i czy można je pomyślnie odzyskać, warto rozważyć rozpoczęcie sprawdzania poprawności natychmiast po utworzeniu kopii zapasowej.

2. **Elementy do sprawdzenia poprawności** — wybierz sprawdzanie poprawności całego archiwum lub ostatniej kopii zapasowej w tym archiwum. Sprawdzanie poprawności kopii zapasowej plików symuluje odzyskiwanie wszystkich plików z kopii zapasowej do tymczasowego miejsca docelowego. Sprawdzanie poprawności kopii zapasowej woluminu polega na obliczeniu sumy kontrolnej wszystkich bloków danych zapisanych w kopii zapasowej. Sprawdzanie poprawności archiwum oznacza sprawdzenie poprawności wszystkich kopii zapasowych tego archiwum i może zająć dużo czasu oraz korzystać z dużej ilości zasobów systemu.
3. **Harmonogram sprawdzania poprawności** (pojawia się wyłącznie po wybraniu opcji Według harmonogramu w kroku 1) — określ harmonogram sprawdzania poprawności. Więcej informacji znajduje się w sekcji Tworzenie harmonogramu (s. 185).

6.2.13 Konfigurowanie regularnej konwersji na maszynę wirtualną

Podczas definiowania planu tworzenia kopii zapasowych (s. 219) można skonfigurować regularną konwersję kopii zapasowej dysku lub woluminu na maszynę wirtualną. W tej sekcji znajdują się informacje, które umożliwiają wprowadzenie odpowiednich ustawień.

Konfigurowanie harmonogramu konwersji

Kopia zapasowa dysku (s. 424) utworzona podczas wykonywania planu tworzenia kopii zapasowych może zostać przekonwertowana na maszynę wirtualną natychmiast, według harmonogramu, lub przy użyciu obu tych metod.

Zadanie konwersji zostanie utworzone na komputerze, którego dotyczy tworzenie kopii zapasowej, i użyje daty oraz godziny tego komputera.

W wyniku pierwszej konwersji tworzona jest nowa maszyna wirtualna. Każda kolejna konwersja powoduje ponowne utworzenie tej maszyny od podstaw. Na początku tworzona jest nowa (tymczasowa) maszyna wirtualna. Jeśli ta operacja zakończy się powodzeniem, poprzednia maszyna jest zastępowana. Jeśli w czasie tworzenia tymczasowej maszyny wystąpi błąd, jest ona usuwana. Oznacza to, że rezultatem wykonania zadania zawsze jest jedna maszyna wirtualna. Jednak podczas konwersji wymagane jest dodatkowe miejsce, tak aby zmieściła się także maszyna tymczasowa.

Podczas konwersji stara maszyna wirtualna musi być wyłączona. W przeciwnym razie nie będzie można jej usunąć i zadanie konwersji zakończy się niepowodzeniem. W takiej sytuacji należy wyłączyć maszynę i ręcznie ponownie uruchomić zadanie konwersji. Wszystkie zmiany wprowadzone we włączonej maszynie zostaną zastąpione.

Wybieranie hosta wykonującego konwersję

Określ komputer, który wykona konwersję. Na komputerze musi być zainstalowany Acronis Backup & Recovery 10 Agent dla systemu Windows, Agent dla ESX/ESXi lub Agent dla Hyper-V.

Należy rozważyć poniższe czynniki.

Jaki agent jest zainstalowany na hoście?

Typ i lokalizacja wynikowej maszyny wirtualnej zależą od agenta znajdującego się na wybranym hoście.

- Na hoście jest zainstalowany **agent dla systemu Windows**

Dostępne są następujące typy maszyn wirtualnych: VMware Workstation, Microsoft Virtual PC lub Parallels Workstation. Pliki nowej maszyny wirtualnej zostaną umieszczane w wybranym folderze.

- Na hoście jest zainstalowany **agent dla ESX/ESXi**

  Na serwerze ESX/ESXi zostanie utworzona maszyna wirtualna VMware.

  Maszyny wirtualne powstałe w wyniku operacji tworzenia kopii zapasowych nie powinny być uwzględniane w kolejnych takich operacjach. Z tego powodu nie są one wyświetlane na serwerze zarządzania, chyba że została włączona integracja z serwerem VMware vCenter Server. W przypadku włączenia integracji maszyny tego typu są wyświetlane jako niemożliwe do zarządzania. Nie można do nich zastosować zasad tworzenia kopii zapasowych.

- Na hoście jest zainstalowany **agent dla Hyper-V**

  Można utworzyć maszynę wirtualną na serwerze Hyper-V albo maszynę wirtualną VMware Workstation, Microsoft Virtual PC lub Parallels Workstation w wybranym folderze.

  Maszyny wirtualne utworzone na serwerze Hyper-V na skutek operacji tworzenia kopii zapasowych nie pojawią się na serwerze zarządzania. Wynika to z faktu, że maszyny tego typu nie powinny być umieszczane w kopiach zapasowych.

Jaka jest moc obliczeniowa hosta?

Zadanie konwersji zostanie utworzone na komputerze, którego dotyczy tworzenie kopii zapasowej, i użyje daty oraz godziny tego komputera. W rzeczywistości zadanie to zostanie wykonane przez wybranego hosta i wykorzysta moc obliczeniową jego procesora. Jeśli host realizuje wiele planów tworzenia kopii zapasowych, może na nim powstać kolejka zadań konwersji. Ich wykonanie może potrwać długi czas.

Jaki magazyn będzie używany przez maszyny wirtualne?

Wykorzystanie sieci

W przeciwieństwie do zwykłych kopii zapasowych (plików TIB) pliki maszyn wirtualnych są przesyłane przez sieć w postaci nieskompresowanej. Oznacza to, że z punktu widzenia wykorzystania sieci optymalnym rozwiązaniem jest użycie sieci SAN lub magazynu lokalnego względem hosta, który wykonuje konwersję. Jeśli jednak konwersja jest wykonywana przez ten sam komputer, którego dotyczy operacja tworzenia kopii zapasowej, nie można użyć dysku lokalnego. Warto wówczas skorzystać z urządzenia NAS.

Miejsce na dysku

W systemie VMware ESX/ESXi nowe maszyny są tworzone ze wstępnie przydzielonymi dyskami. Oznacza to, że rozmiar dysku wirtualnego jest zawsze równy pojemności oryginalnego dysku. Jeśli oryginalny dysk ma pojemność 100 GB, odpowiadający mu dysk wirtualny także zajmie 100 GB, nawet jeśli będzie zawierał 10 GB danych.

Maszyny wirtualne tworzone na serwerze Hyper-V oraz maszyny typu stacja robocza (VMware Workstation, Microsoft Virtual PC lub Parallels Workstation) wykorzystują tyle miejsca na dysku, ile zajmują oryginalne dane. Ponieważ miejsce nie jest wstępnie przydzielane, na dysku fizycznym, na którym będzie działała maszyna wirtualna, powinno być dosyć wolnego miejsca na zwiększenie rozmiarów dysków wirtualnych.

6.3 Odzyskiwanie danych

W przypadku odzyskiwania danych należy najpierw rozważyć metodę najbardziej funkcjonalną: podłączenie konsoli do **komputera zarządzanego działającego pod kontrolą systemu operacyjnego** i utworzenie zadania odzyskiwania.

Jeśli na komputerze zarządzanym **system operacyjny nie uruchomi się** lub konieczne będzie odzyskanie danych **na komputer bez systemu operacyjnego**, uruchom komputer z nośnika startowego (s. 424) lub przy użyciu programu Acronis Startup Recovery Manager (s. 61). Następnie utwórz zadanie odzyskiwania.

Narzędzie Acronis Universal Restore (s. 62)umożliwia odzyskiwanie danych i uruchamianie **systemu Windows na komputerze o innej konfiguracji sprzętowej** lub na maszynie wirtualnej.

System Windows może zostać uruchomiony w ciągu kilku sekund — jeszcze podczas jego odzyskiwania. Korzystając z własnej technologii Acronis Active Restore (s. 63), program Acronis Backup & Recovery 10 uruchamia na komputerze system operacyjny znaleziony w kopii zapasowej, tak jakby system znajdował się na dysku fizycznym. System odzyskuje sprawność i może udostępniać niezbędne usługi. W ten sposób czas przestoju systemu jest minimalny.

Wolumin dynamiczny można odzyskać na istniejący wolumin, nieprzydzielone miejsce grupy dysków lub nieprzydzielone miejsce dysku podstawowego. Aby uzyskać więcej informacji na temat odzyskiwania woluminów dynamicznych, zobacz Microsoft LDM (woluminy dynamiczne) (s. 48).

Komponent Acronis Backup & Recovery 10 Agent dla systemu Windows umożliwia odzyskanie kopii zapasowej dysku (woluminu) na nową maszynę wirtualną jednego z następujących typów: VMware Workstation, Microsoft Virtual PC, Parallels Workstation, Citrix XenServer Open Virtual Appliance (OVA) lub Red Hat KVM. Urządzenie wirtualne można następnie zaimportować na serwer XenServer. Stację roboczą VMware można przekonwertować na otwarty format wirtualizacji (ang. open virtualization format, OVF) przy użyciu narzędzia VMware OVF. Komponent Acronis Backup & Recovery 10 Agent for Hyper-V lub Agent for ESX/ESXi umożliwia utworzenie nowej maszyny wirtualnej na odpowiednim serwerze wirtualizacji.

Przed odzyskiwaniem może być konieczne przygotowanie dysków docelowych. Program Acronis Backup & Recovery 10 zawiera wygodne narzędzie do zarządzania dyskami, które umożliwia tworzenie i usuwanie woluminów, zmianę stylu partycjonowania dysku, tworzenie grupy dysków oraz wykonywanie innych operacji zarządzania dyskami w docelowej konfiguracji sprzętowej, zarówno z poziomu systemu operacyjnego, jak i na komputerze bez systemu. Aby uzyskać więcej informacji na temat narzędzia Acronis Disk Director LV, zobacz Zarządzanie dyskami (s. 309).

Aby utworzyć zadanie odzyskiwania, wykonaj poniższe czynności

Ogólne

Nazwa zadania

[Opcjonalnie] Wprowadź unikatową nazwę zadania odzyskiwania. Dobrze dobrana nazwa umożliwi szybką identyfikację zadania pośród innych zadań.

Poświadczenia zadania (s. 252)

[Opcjonalnie] Zadanie będzie uruchamiane w imieniu użytkownika, który je utworzył. W razie potrzeby można zmienić poświadczenia konta zadania. Aby uzyskać dostęp do tej opcji, zaznacz pole wyboru **Widok zaawansowany**.

Elementy do odzyskania

Archiwum (s. 252)

Wybierz archiwum zawierające dane do odzyskania.

Typ danych (s. 253)

Dotyczy: odzyskiwania dysku

Wybierz typ danych do odzyskania z wybranej kopii zapasowej dysku.

Zawartość (s. 253)

Wybierz kopię zapasową i zawartość do odzyskania.

Poświadczenia dostępu (s. 254)

[Opcjonalnie] Podaj poświadczenia dla lokalizacji archiwum, jeśli konto zadania nie ma praw dostępu do tej lokalizacji. Aby uzyskać dostęp do tej opcji, zaznacz pole wyboru **Widok zaawansowany**.

Lokalizacja odzyskiwania

Ta sekcja pojawia się po wybraniu wymaganej kopii zapasowej i zdefiniowaniu typu danych do odzyskania. Parametry określane tutaj zależą od typu odzyskiwanych danych.

Dyski

Woluminy

Funkcja Acronis Active Restore

[OPCJONALNIE] Pole wyboru **Acronis Active Restore** jest dostępne w przypadku odzyskiwania systemu Windows począwszy od wersji Windows 2000. Funkcja Acronis Active Restore przywraca dostępność systemu niezwłocznie po rozpoczęciu jego odzyskiwania. System operacyjny jest uruchamiany z obrazu kopii zapasowej, a komputer odzyskuje sprawność i może udostępniać niezbędne usługi. Najwyższy priorytet odzyskiwania mają dane umożliwiające obsługę żądań przychodzących. Reszta danych jest odzyskiwana w tle.

Aby uzyskać szczegółowe informacje, zobacz Acronis Active Restore (s. 63).

Pliki (s. 260)

Konieczne może być określenie poświadczeń dla miejsca docelowego. Ten krok należy pominąć w przypadku pracy na komputerze uruchamianym z nośnika startowego.

Poświadczenia dostępu (s. 262)

[Opcjonalnie] Podaj poświadczenia dla miejsca docelowego, jeśli poświadczenia zadania nie umożliwiają odzyskania wybranych danych. Aby uzyskać dostęp do tej opcji, zaznacz pole wyboru **Widok zaawansowany**.

Czas odzyskiwania

Odzyskaj (s. 262)

Wybierz czas rozpoczęcia odzyskiwania. Zadanie można uruchomić niezwłocznie po jego utworzeniu, zaplanować na określoną datę i godzinę w przyszłości lub jedynie zapisać w celu ręcznego wykonania.

[Opcjonalnie] Acronis Universal Restore

Dotyczy: odzyskiwania systemu operacyjnego Windows i woluminu systemowego

Universal Restore (s. 262)

Narzędzia Acronis Universal Restore należy użyć, gdy konieczne jest odzyskanie i uruchomienie systemu Windows na komputerze o innej konfiguracji sprzętowej.

Automatyczne wyszukiwanie sterowników

Określ, gdzie program powinien szukać sterowników warstwy HAL, pamięci masowej i kart sieciowych. Funkcja Acronis Universal Restore zainstaluje sterowniki lepiej dopasowane do docelowej konfiguracji sprzętowej.

Sterowniki pamięci masowej do zainstalowania

[Opcjonalnie] Określ sterowniki pamięci masowej ręcznie, jeśli automatyczne wyszukiwanie sterowników nie powiodło się. Aby uzyskać dostęp do tej opcji, zaznacz pole wyboru **Widok zaawansowany**.

Opcje odzyskiwania

Ustawienia

[Opcjonalnie] Dostosuj operację odzyskiwania, konfigurując odpowiednie opcje, takie jak polecenia poprzedzające/następujące po odzyskiwaniu, priorytet odzyskiwania, obsługa błędów lub opcje powiadomień. Jeśli w tej sekcji nie wykonasz żadnej czynności, zostaną użyte wartości domyślne (s. 134).

Po zmianie dowolnego z ustawień na wartość różną od domyślnej pojawi się nowy wiersz zawierający nowo skonfigurowaną wartość. Stan ustawienia zmieni się z wartości **Domyślne** na **Niestandardowe**. W razie ponownej zmiany ustawienia w wierszu pojawi się nowa wartość, o ile nie będzie to wartość domyślna. W przypadku wartości domyślnej wiersz zniknie. Dlatego w sekcji **Ustawienia** wyświetlane są tylko ustawienia różne od domyślnych.

Kliknięcie **Przywróć domyślne** powoduje przywrócenie wartości domyślnych wszystkich ustawień.

Po wykonaniu wszystkich wymaganych czynności kliknij **OK**, aby zatwierdzić utworzenie zadania odzyskiwania.

6.3.1 Poświadczenia zadania

Określ poświadczenia konta, na którym zadanie będzie uruchamiane.

Aby określić poświadczenia

1. Wybierz jedną z następujących opcji:
   - **Użyj poświadczeń bieżącego użytkownika**

     Zadanie będzie uruchamiane przy użyciu poświadczeń, z którymi zalogował się użytkownik rozpoczynający zadania. Jeśli zadanie ma zostać uruchomione według harmonogramu, w momencie zakończenia tworzenia zadania użytkownik zostanie poproszony o aktualne hasło użytkownika.
   - **Użyj następujących poświadczeń**

     Zadanie będzie zawsze uruchamiane przy użyciu poświadczeń określonych przez użytkownika, niezależnie od tego, czy zadanie będzie uruchamiane ręcznie, czy wykonywane według harmonogramu.

     Określ:
     - **Nazwa użytkownika**. Wprowadzając nazwę konta użytkownika usługi Active Directory, należy określić również nazwę domeny (DOMENA\Nazwa_użytkownika lub Nazwa_użytkownika@domena).
     - **Hasło**. Hasło dla konta.
2. Kliknij **OK**.

Więcej informacji na temat używania poświadczeń w programie Acronis Backup & Recovery 10 można znaleźć w sekcji Właściciele i poświadczenia (s. 35).

Aby dowiedzieć się więcej na temat operacji dostępnych w zależności od uprawnień użytkownika, zobacz sekcję Uprawnienia użytkownika na komputerze zarządzanym (s. 34).

6.3.2 Wybór archiwum

Wybieranie archiwum

1. Wprowadź pełną ścieżkę do lokalizacji w polu **Ścieżka** lub wybierz odpowiedni folder w drzewie folderów.
   - Jeśli archiwum znajduje się w magazynie Acronis Online Backup Storage, kliknij **Zaloguj** i określ poświadczenia logowania do magazynu online. Następnie rozwiń grupę **Magazyn kopii zapasowych online** i wybierz konto.

   W przypadku kopii zapasowych zapisanych w magazynie Acronis Online Backup Storage nie są obsługiwane operacje eksportowania i montowania.

   - Jeśli archiwum znajduje się w skarbcu centralnym, rozwiń grupę **Centralne** i kliknij skarbiec.
   - Jeśli archiwum znajduje się w skarbcu osobistym, rozwiń grupę **Osobiste** i kliknij skarbiec.
   - Jeśli archiwum znajduje się w folderze lokalnym na komputerze, rozwiń grupę **Foldery lokalne** i kliknij odpowiedni folder.

   Jeśli archiwum znajduje się na nośniku wymiennym, na przykład na płycie DVD, najpierw włóż ostatnią płytę DVD, a następnie zgodnie z wyświetlanymi monitami wkładaj kolejno pozostałe płyty, zaczynając od pierwszej.

   - Jeśli archiwum znajduje się w udziale sieciowym, rozwiń grupę **Foldery sieciowe**, wybierz żądany komputer sieciowy, a następnie kliknij folder udostępniony. Jeśli udział sieciowy wymaga poświadczeń dostępu, program wyświetli odpowiedni monit.

   ***Uwaga dla użytkowników systemu Linux:** Aby określić udział sieciowy CIFS (Common Internet File System) zamontowany w punkcie montowania, takim jak /mnt/share, należy wybrać ten punkt montowania, a nie sam udział sieciowy.*

   - Jeśli archiwum znajduje się na serwerze **FTP** lub **SFTP**, w polu **Ścieżka** wpisz nazwę lub adres serwera w następujący sposób:

     ftp://serwer_ftp:numer_portu lub sftp://serwer_sftp:numer_portu

     Jeśli nie określisz numeru portu, dla serwera FTP zostanie użyty port 21, a dla SFTP — 22.

     Po wprowadzeniu poświadczeń dostępu zostaną udostępnione foldery na serwerze. Kliknij odpowiedni folder.

     Dostęp do serwera można uzyskać jako użytkownik anonimowy, o ile serwer zezwala na taki dostęp. W tym celu nie trzeba wprowadzać poświadczeń, lecz należy kliknąć opcję **Użyj dostępu anonimowego**.

   Jak wynika z oryginalnej specyfikacji protokołu FTP, poświadczenia wymagane do uzyskania dostępu do serwerów FTP są przesyłane w sieci jako otwarty tekst. Oznacza to, że nazwę użytkownika i hasło można przejąć przy użyciu programu do przechwytywania pakietów.

   - Jeśli archiwum znajduje się na podłączonym lokalnie urządzeniu taśmowym, rozwiń grupę **Napędy taśmowe** i kliknij odpowiednie urządzenie.

   W przypadku pracy na komputerze uruchamianym z nośnika startowego:

   - Aby uzyskać dostęp do skarbca zarządzanego, w polu **Ścieżka** wpisz następujący ciąg:

     bsp://adres_węzła/nazwa_skarbca/

- Aby uzyskać dostęp do niezarządzanego skarbca centralnego, wpisz pełną ścieżkę do folderu skarbca.

2. Wybierz archiwum w tabeli po prawej stronie drzewa. Tabela przedstawia nazwy archiwów znajdujących się w każdym wybranym przez użytkownika skarbcu lub folderze.

   Gdy przeglądasz zawartość lokalizacji, inni użytkownicy lub sam program mogą dodać, usunąć lub zmodyfikować archiwa. Przycisk **Odśwież** pozwala odświeżyć listę archiwów.
3. Kliknij **OK**.

6.3.3 Typ danych

Wybierz typ danych do odzyskania z wybranej kopii zapasowej dysku:

- **Dyski** — aby odzyskać dyski,
- **Woluminy** — aby odzyskać woluminy,
- **Pliki** — aby odzyskać określone pliki i foldery.

6.3.4 Wybór zawartości

Wygląd tego okna zależy od typu danych przechowywanych w archiwum.

Wybór dysków / woluminów

Aby wybrać kopię zapasową i dyski/woluminy do odzyskania:

1. Wybierz jedną z kolejnych kopii zapasowych na podstawie daty i godziny jej utworzenia. Umożliwi to przywrócenie danych dysku do stanu z określonego momentu.

   Określ elementy do odzyskania. Domyślnie zostaną zaznaczone wszystkie elementy wybranej kopii zapasowej. Jeśli nie chcesz odzyskać niektórych elementów, usuń ich zaznaczenie.
   Aby uzyskać informacje dotyczące dysku/woluminu, kliknij go prawym przyciskiem myszy, a następnie kliknij **Informacje**.
2. Kliknij **OK**.

Wybieranie głównego rekordu rozruchowego

Rekord MBR dysku jest zwykle wybierany, gdy:

- nie można uruchomić systemu operacyjnego;
- dysk jest nowy i nie ma rekordu MBR;
- odzyskiwanie dotyczy startowych programów ładujących: niestandardowych oraz innych niż z systemu Windows (takich jak LILO i GRUB);
- geometria dysku jest inna niż dysku, którego dane są przechowywane w kopii zapasowej.

Prawdopodobnie konieczność odzyskania rekordu MBR wystąpi również przy innej okazji, ale sytuacja powyżej jest najczęstsza.

Odzyskując rekord MBR jednego dysku na inny, program Acronis Backup & Recovery 10 odzyskuje ścieżkę 0, która nie zmienia tabeli ani układu partycji dysku docelowego. Program Acronis Backup & Recovery 10 automatycznie zaktualizuje programy ładujące systemu Windows po zakończeniu operacji odzyskiwania, dlatego nie ma potrzeby odzyskiwania rekordu MBR ani ścieżki 0 w systemach Windows, o ile rekord MBR nie został uszkodzony.

Wybór plików

Aby wybrać kopię zapasową i pliki do odzyskania:

1. Wybierz jedną z kolejnych kopii zapasowych na podstawie daty/godziny jej utworzenia. Umożliwi to przywrócenie plików/folderów do stanu z określonego momentu.
2. Określ pliki i foldery do odzyskania, zaznaczając odpowiadające im pola wyboru w drzewie archiwów.

   Wybór folderu powoduje automatyczne zaznaczenie wszystkich zagnieżdżonych w nim folderów i plików.

   Tabela po prawej stronie drzewa archiwów umożliwia wybieranie elementów zagnieżdżonych. Zaznaczenie pola wyboru obok nagłówka kolumny **Nazwa** powoduje automatyczne zaznaczenie wszystkich elementów w tabeli. Wyczyszczenie tego pola wyboru powoduje automatyczne usunięcie zaznaczenia wszystkich elementów.
3. Kliknij **OK**.

6.3.5 Poświadczenia dostępu do lokalizacji

Określ poświadczenia wymagane w celu dostępu do lokalizacji przechowywania kopii zapasowych.

Aby określić poświadczenia

1. Wybierz jedną z następujących opcji:
   - **Użyj poświadczeń zadania**

     Program użyje poświadczeń konta zadania określonych w sekcji Ogólne w celu dostępu do lokalizacji.
   - **Użyj następujących poświadczeń**

     Program uzyska dostęp do lokalizacji przy użyciu określonych poświadczeń. Tej opcji należy użyć, gdy konto zadania nie ma uprawnień dostępu do lokalizacji. Konieczne może być podanie specjalnych poświadczeń dla udziału sieciowego lub skarbca węzła magazynowania.

     Określ:
     - **Nazwa użytkownika**. Wprowadzając nazwę konta użytkownika usługi Active Directory, należy określić również nazwę domeny (DOMENA\Nazwa_użytkownika lub Nazwa_użytkownika@domena).
     - **Hasło**. Hasło dla konta.
2. Kliknij **OK**.

Jak wynika z oryginalnej specyfikacji protokołu FTP, poświadczenia wymagane do uzyskania dostępu do serwerów FTP są przesyłane w sieci jako otwarty tekst. Oznacza to, że nazwę użytkownika i hasło można przejąć przy użyciu programu do przechwytywania pakietów.

6.3.6 Wybór miejsca docelowego

Określ miejsce docelowe odzyskiwania wybranych danych.

Dyski

Dostępne miejsca docelowe na dyskach zależą od agentów uruchomionych na komputerze.

Odzyskaj do:

Komputer fizyczny

Opcja dostępna, gdy jest zainstalowany komponent Acronis Backup & Recovery 10 Agent for Windows lub Agent for Linux.

Wybrane dyski zostaną odzyskane na dyski fizyczne komputera, do którego jest podłączona konsola. Po wybraniu tej opcji należy wykonać standardową procedurę mapowania dysków opisaną poniżej.

Nowa maszyna wirtualna (s. 259)

Jeśli jest zainstalowany komponent Acronis Backup & Recovery 10 Agent for Windows.

Wybrane dyski zostaną odzyskane na nową maszynę wirtualną jednego z następujących typów: VMware Workstation, Microsoft Virtual PC, Parallels Workstation, Citrix XenServer Open Virtual Appliance (OVA) lub Red Hat KVM. Pliki maszyny wirtualnej zostaną zapisane w określonym miejscu docelowym.

Jeśli jest zainstalowany komponent Acronis Backup & Recovery 10 Agent for Hyper-V lub Agent for ESX/ESXi.

Są to agenty umożliwiające utworzenie nowej maszyny wirtualnej na określonym serwerze wirtualizacji.

Nowa maszyna wirtualna zostanie skonfigurowana automatycznie — w miarę możliwości zostaną skopiowane ustawienia konfiguracji maszyny źródłowej. Konfiguracja zostanie wyświetlona w sekcji **Ustawienia maszyn wirtualnych** (s. 259). Sprawdź te ustawienia i w razie potrzeby wprowadź w nich zmiany.

Następnie wykonaj standardową procedurę mapowania dysków opisaną poniżej.

Istniejąca maszyna wirtualna

Opcja dostępna, gdy jest zainstalowany komponent Acronis Backup & Recovery 10 Agent for Hyper-V lub Agent for ESX/ESXi.

Wybierając tę opcję, należy określić serwer wirtualizacji i docelową maszynę wirtualną. Następnie wykonaj standardową procedurę mapowania dysków opisaną poniżej.

Należy pamiętać, że przed rozpoczęciem odzyskiwania maszyna docelowa zostanie automatycznie wyłączona. Aby wyłączyć ją ręcznie, należy zmienić ustawienie opcji zarządzania zasilaniem maszyny wirtualnej.

Nr dysku:

Nr dysku (MODEL) (s. 258)

Wybierz dysk docelowy dla każdego z dysków źródłowych.

Podpis NT (s. 256)

Wybierz sposób obsługi podpisu odzyskanego dysku. Podpis dysku jest używany w systemie Windows i jądrach systemu Linux w wersji 2.6 lub nowszej.

Dysk docelowy

Aby określić dysk docelowy:

1. Wybierz dysk, na który chcesz odzyskać wybrany dysk. Rozmiar dysku docelowego powinien być co najmniej taki sam, jak rozmiar nieskompresowanych danych w obrazie.
2. Kliknij **OK**.

Wszystkie dane przechowywane na dysku docelowym zostaną zastąpione danymi z kopii zapasowej, dlatego należy zachować ostrożność i uważać, aby nie utracić potrzebnych danych, których nie ma w kopii zapasowej.

Podpis NT

Gdy wraz z kopią zapasową dysku zostanie wybrany główny rekord rozruchowy (MBR), trzeba zachować możliwość uruchamiania systemu operacyjnego na woluminie dysku docelowego. W systemie operacyjnym informacje o woluminie systemowym (na przykład litera woluminu) muszą pasować do podpisu NT dysku, przechowywanego w jego rekordzie MBR. Ale dwa dyski o tym samym podpisie NT nie mogą działać prawidłowo w jednym systemie operacyjnym.

Jeśli dwa dyski w komputerze mają ten sam podpis NT i zawierają wolumin systemowy, podczas rozruchu system operacyjny uruchamia się z pierwszego dysku, wykrywa taki sam podpis na drugim dysku, automatycznie generuje nowy, unikatowy podpis NT i przypisuje go do drugiego dysku. Skutkiem tego wszystkie woluminy na drugim dysku tracą swoje litery, wszystkie ścieżki na dysku stają się nieprawidłowe, a programy nie mogą znaleźć swoich plików. Uruchomienie systemu operacyjnego umieszczonego na tym dysku jest niemożliwe.

Aby zachować możliwość uruchamiania systemu na woluminie dysku docelowego, wybierz jedną z następujących opcji:

- **Wybierz automatycznie**

  Nowy podpis NT zostanie utworzony tylko wówczas, gdy istniejący podpis różni się od podpisu w kopii zapasowej. W przeciwnym razie zostanie zachowany istniejący podpis NT.

- **Utwórz nowy**

  Program utworzy nowy podpis NT docelowego dysku twardego.

- **Odzyskaj z kopii zapasowej**

  Program zastąpi podpis NT docelowego dysku twardego podpisem z kopii zapasowej dysku.

  Odzyskanie podpisu dysku może być pożądane z następujących przyczyn:

  - Program Acronis Backup & Recovery 10 tworzy zaplanowane zadania przy użyciu podpisu źródłowego dysku twardego. W przypadku odzyskania tego samego podpisu dysku nie trzeba ponownie tworzyć ani edytować utworzonych wcześniej zadań.
  - Niektóre zainstalowane aplikacje używają podpisu dysku do przydzielania licencji i w innych celach.
  - Umożliwia zachowanie wszystkich punktów przywracania systemu Windows na odzyskanym dysku.
  - Umożliwia odzyskanie migawek usługi kopiowania woluminów w tle używanej przez funkcję „Poprzednie wersje” w systemie Windows Vista.

- **Zachowaj istniejący**

  Program zachowa bez zmian istniejący podpis NT docelowego dysku twardego.

Woluminy

Dostępne miejsca docelowe woluminów zależą od agentów uruchomionych na komputerze.

Odzyskaj do:

Komputer fizyczny

Opcja dostępna, gdy jest zainstalowany komponent Acronis Backup & Recovery 10 Agent dla systemu Windows lub Agent dla systemu Linux.

Wybrane woluminy zostaną odzyskane na dyski fizyczne komputera, do którego jest podłączona konsola. Po wybraniu tej opcji należy wykonać standardową procedurę mapowania dysków opisaną poniżej.

Nowa maszyna wirtualna (s. 259)

Jeśli jest zainstalowany komponent Acronis Backup & Recovery 10 Agent dla systemu Windows.

Wybrane woluminy zostaną odzyskane na nową maszynę wirtualną jednego z następujących typów: VMware Workstation, Microsoft Virtual PC, Parallels Workstation, Citrix XenServer Open Virtual Appliance (OVA) lub Red Hat KVM. Pliki maszyny wirtualnej zostaną zapisane w określonym miejscu docelowym.

Jeśli jest zainstalowany komponent Acronis Backup & Recovery 10 Agent dla Hyper-V lub Agent dla ESX/ESXi.

Są to agenty umożliwiające utworzenie nowej maszyny wirtualnej na określonym serwerze wirtualizacji.

Nowa maszyna wirtualna zostanie skonfigurowana automatycznie — w miarę możliwości zostaną skopiowane ustawienia konfiguracji maszyny źródłowej. Konfiguracja zostanie wyświetlona w sekcji **Ustawienia maszyn wirtualnych** (s. 259). Sprawdź te ustawienia i w razie potrzeby wprowadź w nich zmiany.

Następnie należy wykonać standardową procedurę mapowania woluminów opisaną poniżej.

Istniejąca maszyna wirtualna

Opcja dostępna, gdy jest zainstalowany komponent Acronis Backup & Recovery 10 Agent dla Hyper-V lub Agent dla ESX/ESXi.

Wybierając tę opcję, należy określić serwer wirtualizacji i docelową maszynę wirtualną. Następnie należy wykonać standardową procedurę mapowania woluminów opisaną poniżej.

Należy pamiętać, że przed rozpoczęciem odzyskiwania maszyna docelowa zostanie automatycznie wyłączona. Aby wyłączyć ją ręcznie, należy zmienić ustawienie opcji zarządzania zasilaniem maszyny wirtualnej.

Odzyskaj MBR dysku [nr dysku] na: [Jeśli wybrano odzyskiwanie głównego rekordu startowego]

Nr dysku (s. 257)

Wybierz dysk, na który chcesz odzyskać główny rekord startowy.

Podpis NT: (s. 256)

Wybierz sposób obsługi podpisu dysku umieszczonego w głównym rekordzie startowym. Podpis dysku jest używany w systemie Windows i jądrach systemu Linux w wersji 2.6 lub nowszej.

Odzyskaj [wolumin] [litera] na:

Nr dysku/Wolumin (s. 258)

Mapowanie kolejno wszystkich woluminów źródłowych na wolumin lub nieprzydzielone miejsce na dysku docelowym.

Rozmiar:

[Opcjonalnie] Zmień rozmiar, lokalizację i inne właściwości odzyskanego woluminu.

Miejsce docelowe rekordu MBR

Aby określić dysk docelowy:

1. Wybierz dysk, na który chcesz odzyskać rekord MBR.
2. Kliknij **OK**.

Miejsce docelowe woluminu

Aby określić wolumin docelowy:

1. Wybierz wolumin lub nieprzydzielone miejsce, gdzie wybrany wolumin ma zostać odzyskany. Docelowy wolumin lub docelowe nieprzydzielone miejsce powinny mieć przynajmniej taki sam rozmiar jak obraz danych nieskompresowanych.
2. Kliknij **OK**.

Wszystkie dane przechowywane w woluminie docelowym zostaną zastąpione danymi kopii zapasowej, tak więc należy zachować ostrożność i uważać na dane, które nie mają kopii zapasowej, a mogą być potrzebne.

W przypadku korzystania z nośnika startowego

Litery dysków widoczne podczas pracy na nośniku startowym w stylu systemu Windows mogą się różnić od sposobu identyfikacji dysków przez system Windows. Na przykład dysk D: w narzędziu ratunkowym może odpowiadać dyskowi E: w systemie Windows.

Należy zachować ostrożność! Dla bezpieczeństwa zaleca się przypisywanie unikatowych nazw do woluminów.

Na nośnikach startowych w stylu systemu Linux dyski i woluminy lokalne są pokazywane jako odmontowane (sda1, sda2...).

Właściwości woluminów

Zmiana rozmiaru i przeniesienie

W procesie odzyskiwania woluminu na standardowy dysk MBR można zmienić rozmiar i umiejscowienie woluminu, przeciągając go lub jego krawędzie myszą albo wprowadzając odpowiednie wartości we właściwych polach. Dzięki tej funkcji można rozłożyć miejsce na dysku między odzyskiwane woluminy. W tym przypadku trzeba najpierw odzyskać wolumin, który będzie zmniejszany.

Wskazówka: *Rozmiaru woluminu nie można zmienić w przypadku jego odzyskiwania z kopii zapasowej podzielonej na kilka płyt DVD lub taśm. Aby zmienić rozmiar woluminu, należy skopiować wszystkie części kopii zapasowej do jednej lokalizacji na dysku twardym.*

Właściwości

Typ

Standardowy dysk MBR może zawierać maksymalnie cztery woluminy podstawowe lub maksymalnie trzy woluminy podstawowe i wiele dysków logicznych. Program domyślnie wybiera oryginalny typ woluminu. W razie potrzeby to ustawienie można zmienić.

- **Podstawowy**. Informacje dotyczące woluminów podstawowych znajdują się w tabeli partycji MBR. Większość systemów operacyjnych można uruchomić tylko z woluminu podstawowego pierwszego dysku twardego, ale liczba woluminów podstawowych jest ograniczona.

  Chcąc odzyskać wolumin systemowy na standardowy dysk MBR, zaznacz pole wyboru Aktywny. Wolumin aktywny jest używany do ładowania systemu operacyjnego. Wybór opcji Aktywny w przypadku woluminu bez zainstalowanego systemu operacyjnego może uniemożliwić uruchomienie komputera. Dysku logicznego ani woluminu dynamicznego nie można ustawić jako aktywnego.
- **Logiczny**. Informacje dotyczące woluminów logicznych znajdują się nie w głównym rekordzie startowym, ale w tablicy partycji rozszerzonej. Liczba woluminów logicznych na dysku jest

nieograniczona. Woluminu logicznego nie można ustawić jako aktywnego. W przypadku odzyskiwania woluminu systemowego na inny dysk twardy, który zawiera własne woluminy i system operacyjny, najczęściej potrzebne są tylko dane. W takiej sytuacji można odzyskać wolumin jako logiczny, aby uzyskać dostęp do samych danych.

System plików

W razie potrzeby zmień system plików woluminu. Program domyślnie wybiera system plików oryginalnego woluminu. Program Acronis Backup & Recovery 10 umożliwia następujące rodzaje konwersji między systemami plików: FAT 16 -> FAT 32 oraz Ext2 -> Ext3. W przypadku woluminów z innymi macierzystymi systemami plików ta opcja jest niedostępna.

Załóżmy, że wolumin ze starego dysku o małej pojemności z systemem plików FAT16 chcemy odzyskać na nowszy dysk. System plików FAT16 nie będzie skuteczny, co więcej — jego ustawienie na dysku twardym o dużej pojemności może okazać się niemożliwe. Wynika to z faktu, że system plików FAT16 obsługuje woluminy o maksymalnej wielkości 4GB, zatem bez zmiany systemu plików odzyskanie woluminu FAT16 o wielkości 4GB na wolumin przekraczający ten limit jest niemożliwe. W tej sytuacji zaleca się zmianę systemu plików z FAT16 na FAT32.

Starsze systemy operacyjne (MS-DOS, Windows 95 i Windows NT 3.x, 4.x) nie obsługują systemu plików FAT32 i nie będą działały po odzyskaniu woluminu i zmianie jego systemu plików. Można je zwykle odzyskać tylko na wolumin z systemem plików FAT16.

Litera dysku logicznego (tylko Windows)

Przypisz literę do odzyskiwanego woluminu. Wybierz literę z listy rozwijanej.

- Przy domyślnym wyborze AUTO do woluminu zostanie przypisana pierwsza niewykorzystana litera.
- Wybór NIE oznacza nieprzypisanie żadnej litery do odzyskanego woluminu i ukrycie go przed systemem operacyjnym. Nie należy przypisywać liter do woluminów, które są niedostępne dla systemu Windows, takich jak woluminy inne niż FAT i NTFS.

Wybór typu maszyny wirtualnej / serwera wirtualizacji

Nową maszynę wirtualną można utworzyć na serwerze wirtualizacji (wymaga to zainstalowania agenta Acronis Backup & Recovery 10 dla Hyper-V lub ESX/ESXi) lub w dowolnym dostępnym folderze lokalnym lub sieciowym.

Aby wybrać serwer wirtualizacji, na którym program ma utworzyć nową maszynę wirtualną

1. Wybierz **Umieść na wybranym serwerze wirtualizacji**.
2. Wybierz serwer wirtualizacji po lewej stronie okna. Po prawej stronie okna sprawdź szczegółowe informacje na temat serwera.
3. Kliknij **OK**, aby powrócić do strony **Odzyskiwanie danych**.

Aby wybrać typ maszyny wirtualnej

1. Wybierz **Zapisz jako pliki wybranego typu maszyny wirtualnej w określonym folderze**.
2. Wybierz typ maszyny wirtualnej po lewej stronie okna. Po prawej stronie okna sprawdź szczegółowe informacje na temat wybranego typu maszyny wirtualnej.
3. Kliknij **OK**, aby powrócić do strony **Odzyskiwanie danych**.

Ustawienia maszyn wirtualnych

Konfigurować można poniższe ustawienia maszyn wirtualnych.

Magazyn

Ustawienie początkowe: magazyn domyślny serwera wirtualizacji, jeśli nowa maszyna jest tworzona na tym serwerze. W przeciwnym razie jest to folder dokumentów bieżącego użytkownika.

Jest to miejsce, w którym zostanie utworzona nowa maszyna wirtualna. Możliwość zmiany magazynu na serwerze wirtualizacji zależy od producenta oprogramowania do wirtualizacji i jego ustawień. VMware ESX obsługuje wiele magazynów. Serwer Microsoft Hyper-V umożliwia utworzenie nowej maszyny wirtualnej w dowolnym folderze lokalnym.

Pamięć

Ustawienie początkowe: jeśli nie jest zawarte w kopii zapasowej, domyślne ustawienie serwera wirtualizacji.

Jest to ilość pamięci przydzielona nowej maszynie wirtualnej. Zakres regulacji ilości pamięci zależy od sprzętu zainstalowanego w hoście, systemu operacyjnego hosta i ustawień oprogramowania do wirtualizacji. Na przykład maksymalna dozwolona ilość pamięci na potrzeby maszyn wirtualnych może wynosić 30% pamięci całkowitej.

Dyski

Ustawienie początkowe: liczba i rozmiar dysków komputera źródłowego.

Liczba dysków jest zwykle taka sama jak w komputerze źródłowym. Jednak może być inna z powodu ograniczeń narzuconych przez oprogramowanie do wirtualizacji, gdy program musi dodać więcej dysków w celu pomieszczenia woluminów komputera źródłowego. W konfiguracji maszyny można dodać dyski wirtualne, a w niektórych przypadkach usunąć proponowane dyski.

Implementacja maszyn Xen jest oparta na programie Microsoft Virtual PC i ma jego ograniczenia: do 3 dysków IDE i 1 procesor. Dyski SCSI nie są obsługiwane.

Procesory

Ustawienie początkowe: jeśli nie jest zawarte w kopii zapasowej lub ustawienie z kopii zapasowej jest nieobsługiwane przez serwer wirtualizacji, jest to domyślne ustawienie serwera.

Jest to liczba procesorów nowej maszyny wirtualnej. W większości przypadków jest to wartość równa jeden. Efekt przydzielenia maszynie więcej niż jednego procesora nie jest gwarantowany. Liczba procesorów wirtualnych może być ograniczona przez konfigurację procesorów hosta, oprogramowanie do wirtualizacji lub system operacyjny-gościa. Na hostach wieloprocesorowych jest na ogół dostępnych wiele procesorów wirtualnych. Wielordzeniowy procesor hosta lub technologia hyperthreading umożliwiają czasem obsługę wielu procesorów wirtualnych na hoście z jednym procesorem.

Miejsce docelowe pliku

Aby określić miejsce docelowe:

1. Wybierz lokalizację, do której zostaną odzyskane pliki z kopii zapasowej:
   - **Oryginalna lokalizacja** — pliki i foldery zostaną odzyskane do lokalizacji o takiej samej ścieżce lub ścieżkach jak w kopii zapasowej. Jeśli kopie zapasowe wszystkich plików i folderów znajdowały się w C:\Documents\Finance\Reports\, pliki zostaną odzyskane do lokalizacji o takiej samej ścieżce. Jeśli folder nie istnieje, zostanie utworzony automatycznie.

- **Nowa lokalizacja** — pliki zostaną odzyskane do lokalizacji określonej w drzewie. Pliki i foldery zostaną odzyskane bez odtwarzania pełnej ścieżki, chyba że pole wyboru **Odzyskaj bez pełnej ścieżki** będzie wyczyszczone.

2. Kliknij **OK**.

Wykluczenia podczas odzyskiwania

Skonfiguruj wykluczenia określonych plików, których nie chcesz odzyskiwać.

Aby utworzyć listę masek plików, użyj przycisków **Dodaj**, **Edytuj**, **Usuń** i **Usuń wszystko**. Pliki, których nazwy pasują do dowolnej z masek, zostaną pominięte podczas odzyskiwania.

W masce plików można użyć jednego lub kilku symboli wieloznacznych * i ?:

- Gwiazdka (*) zastępuje dowolną liczbę znaków w nazwie pliku (w tym również zero). Na przykład maska Dok*.txt zwraca pliki takie jak Dok.txt i Dokument.txt
- Znak zapytania (?) zastępuje dokładnie jeden znak w nazwie pliku. Na przykład maska Dok?.txt zwraca pliki takie jak Dok1.txt i Doku.txt, ale nie zwraca plików Dok.txt ani Dok11.txt

Przykłady wykluczeń

Kryterium	Przykład	Opis
Windows i Linux		
Według nazwy	F.log F	Wyklucza wszystkie pliki o nazwie „F.log”. Wyklucza wszystkie foldery o nazwie „F”.
Według maski (*)	*.log F*	Wyklucza wszystkie pliki z rozszerzeniem .log. Wyklucza wszystkie pliki i foldery, których nazwa rozpoczyna się od litery „F” (np. foldery F, F1 i pliki F.log, F1.log).
Według maski (?)	F???.log	Wyklucza wszystkie pliki z rozszerzeniem .log, których nazwy składają się z czterech znaków i zaczynają od litery „F”.
Windows		
Według ścieżki pliku	Finanse\F.log	Wyklucza pliki o nazwie „F.log” z wszystkich folderów o nazwie „Finanse”.
Według ścieżki folderu	Finanse\F\ lub Finanse\F	Wyklucza foldery o nazwie „F” z wszystkich folderów o nazwie „Finanse”.
Linux		
Według ścieżki pliku	/home/user/Finanse/F.log	Wyklucza plik „F.log” znajdujący się w folderze /home/user/Finanse.

Powyższe ustawienia nie dotyczą plików lub folderów, które zostały wprost wybrane do odzyskania. Załóżmy, że wybierzesz na przykład folder MojFolder i plik MojPlik.tmp znajdujący się poza tym folderem oraz zdecydujesz o pominięciu wszystkich plików .tmp. W tej sytuacji w trakcie odzyskiwania zostaną pominięte wszystkie pliki .tmp znajdujące się w folderze MojFolder, ale plik MojPlik.tmp nie zostanie pominięty.

Zastępowanie

Określ zachowanie programu, gdy w folderze docelowym znajdzie plik o takiej samej nazwie jak w archiwum:

- **Zastąp istniejący plik** — plik znajdujący się w kopii zapasowej otrzyma pierwszeństwo przed plikiem na dysku twardym.
- **Zastąp istniejący plik, jeśli jest starszy** — pierwszeństwo otrzyma plik zmodyfikowany później, niezależnie od tego, czy znajduje się w kopii zapasowej, czy na dysku.
- **Nie zastępuj istniejącego pliku** — plik znajdujący się na dysku twardym otrzyma pierwszeństwo przed plikiem w kopii zapasowej.

Po zezwoleniu na zastępowanie plików nadal można zapobiec zastępowaniu określonych plików, wykluczając (s. 261) je z operacji odzyskiwania.

6.3.7 Poświadczenia dostępu do miejsca docelowego

Aby określić poświadczenia

1. Wybierz jedno z następujących ustawień:
   - **Użyj poświadczeń zadania**

     Program użyje poświadczeń konta zadania określonych w sekcji Ogólne w celu dostępu do miejsca docelowego.
   - **Użyj następujących poświadczeń**

     Program użyje poświadczeń określonych przez użytkownika w celu dostępu do miejsca docelowego. Użyj tej opcji, jeśli konto zadania nie posiada uprawnień dostępu do miejsca docelowego.

     Określ:
     - **Nazwa użytkownika**. Wprowadzając nazwę konta użytkownika usługi Active Directory, należy określić również nazwę domeny (DOMENA\Nazwa_użytkownika lub Nazwa_użytkownika@domena).
     - **Hasło**. Hasło dla konta.
2. Kliknij **OK**.

6.3.8 Czas odzyskiwania

Wybierz czas rozpoczęcia wykonywania zadania odzyskiwania:

- **Odzyskaj Teraz** — zadanie odzyskiwania rozpocznie się natychmiast po kliknięciu **OK** na końcu procedury.
- **Odzyskaj Później** — zadanie odzyskiwania rozpocznie się w określonym dniu o określonej godzinie.

Jeśli nie chcesz planować rozpoczęcia zadania i chcesz je uruchomić ręcznie, zaznacz pole wyboru **Zadanie zostanie uruchomione ręcznie (nie planuj zadania)**.

6.3.9 Universal Restore

Narzędzia Acronis Universal Restore należy użyć, gdy konieczne jest odzyskanie i uruchomienie systemu Windows na komputerze o innej konfiguracji sprzętowej. Narzędzie Universal Restore niweluje różnice między urządzeniami istotnymi dla uruchamiania systemu operacyjnego, takimi jak kontrolery pamięci, płyta główna i chipset.

Aby dowiedzieć się więcej na temat technologii Universal Restore, zobacz sekcję Universal Restore (s. 62).

Narzędzie Acronis Backup & Recovery 10 Universal Restore jest niedostępne w następujących przypadkach:

- uruchamianie komputera za pomocą programu Acronis Startup Recovery Manager (przez naciśnięcie klawisza F11),
- umiejscowienie obrazu kopii zapasowej w strefie Acronis Secure Zone,
- korzystanie z funkcji Acronis Active Restore (s. 418),

ponieważ są to funkcje przeznaczone głównie do natychmiastowego odzyskiwania danych na tym samym komputerze.

Przygotowanie

Przed odzyskaniem systemu Windows na komputerze o innej konfiguracji sprzętowej upewnij się, że masz sterowniki kontrolera nowego dysku twardego i chipsetu. Sterowniki mają zasadnicze znaczenie dla uruchomienia systemu operacyjnego. Skorzystaj z płyty CD lub DVD dostarczonej przez producenta sprzętu albo pobierz sterowniki z jego witryny internetowej. Pliki sterowników powinny mieć rozszerzenia *.inf, *.sys lub *.oem. Jeśli pobrane sterowniki mają format *.exe, *.cab lub *.zip, rozpakuj je za pomocą oddzielnej aplikacji, na przykład WinRAR (http://www.rarlab.com/) lub Universal Extractor (http://legroom.net/software/uniextract).

Najlepszą praktyką jest przechowywanie sterowników do wszystkich urządzeń używanych w przedsiębiorstwie w jednym repozytorium uporządkowanym według typu urządzenia lub według konfiguracji sprzętowej. Kopię repozytorium można przechowywać na płycie DVD lub dysku flash. Można również wybrać niektóre sterowniki i dodać je do nośnika startowego bądź utworzyć niestandardowy nośnik startowy z koniecznymi sterownikami (oraz niezbędną konfiguracją sieciową) dla każdego serwera. Można również określać ścieżkę do repozytorium podczas każdego korzystania z narzędzia Universal Restore.

Praca z nośnikiem startowym wymaga dostępu do urządzenia ze sterownikami. Nawet w przypadku skonfigurowania odzyskiwania dysku systemowego w środowisku systemu Windows po ponownym uruchomieniu komputera odzyskiwanie będzie przebiegać w środowisku opartym na systemie Linux. Użyj nośnika opartego na środowisku WinPE, jeśli urządzenie jest dostępne w systemie Windows, ale nośnik oparty na systemie Linux go nie wykrywa.

Ustawienia narzędzia Universal Restore

Automatyczne wyszukiwanie sterowników

Określ, gdzie program powinien szukać sterowników warstwy abstrakcji sprzętu (HAL), kontrolera dysku twardego i karty sieciowej:

— Jeśli sterowniki znajdują się na płycie producenta lub innym nośniku wymiennym, włącz funkcję **Przeszukaj nośniki wymienne**.

— Jeśli nośniki znajdują się w folderze sieciowym lub na nośniku startowym, określ ścieżkę do folderu w polu **Przeszukaj folder**.

Podczas odzyskiwania narzędzie Universal Restore wykonuje wyszukiwanie rekursywne we wszystkich podfolderach określonego folderu, znajduje wśród dostępnych sterowników najbardziej odpowiednie sterowniki HAL i kontrolera dysku twardego, a następnie instaluje je w odzyskanym systemie. Narzędzie Universal Restore wyszukuje również sterownik karty sieciowej i przesyła ścieżkę znalezionego sterownika do systemu operacyjnego. Jeśli sprzęt zawiera wiele kart interfejsu sieciowego, narzędzie próbuje skonfigurować sterowniki wszystkich kart. Jeśli

Universal Restore nie znajdzie kompatybilnego sterownika w określonej lokalizacji, określi urządzenie powodujące problem i wyświetli monit o płytę lub ścieżkę sieciową do sterownika.

System Windows po uruchomieniu rozpoczyna standardową procedurę instalowania nowego sprzętu. Jeśli sterownik karty sieciowej ma podpis Microsoft Windows, system instaluje go w trybie dyskretnym. W przeciwnym razie system wyświetla monit o potwierdzenie instalacji niepodpisanego sterownika.

Następnie można skonfigurować połączenie sieciowe i określić sterowniki karty graficznej, złącza USB i innych urządzeń.

Sterowniki pamięci masowej do zainstalowania

Aby uzyskać dostęp do tej opcji, zaznacz pole wyboru **Widok zaawansowany**.

Jeśli docelowy sprzęt zawiera określony kontroler pamięci masowej, na przykład RAID (zwłaszcza NVIDIA RAID) lub kartę Fibre Channel, określ odpowiednie sterowniki w polu **Sterowniki**.

Sterowniki określone w tym miejscu mają pierwszeństwo. Program zainstaluje je z ewentualnymi ostrzeżeniami, nawet jeśli znajdzie lepszy sterownik.

Tej opcji należy użyć tylko wtedy, gdy automatyczne wyszukiwanie sterowników nie pozwoli na uruchomienie systemu.

Sterowniki maszyny wirtualnej

W przypadku odzyskiwania systemu na nową maszynę wirtualną technologia Universal Restore jest stosowana w tle, ponieważ program posiada informacje o sterownikach wymaganych do obsługiwanych maszyn wirtualnych.

Jeśli system jest odzyskiwany na istniejącą maszynę wirtualną używającą kontrolera dysków twardych SCSI, w kroku **Sterowniki pamięci masowej do zainstalowania** wybierz sterowniki SCSI dla środowiska wirtualnego. Użyj sterowników dołączonych do oprogramowania maszyny wirtualnej lub pobierz najnowsze sterowniki z witryny internetowej producenta oprogramowania.

6.3.10 Jak przekonwertować kopię zapasową dysku na maszynę wirtualną

Zamiast konwertowania pliku TIB na plik dysku wirtualnego, który wymaga wykonania kolejnych operacji w celu rozpoczęcia jego używania, program Acronis Backup & Recovery 10 wykonuje konwersję przez odzyskanie kopii zapasowej dysku na nową, w pełni skonfigurowaną i działającą maszynę wirtualną. Podczas operacji odzyskiwania użytkownik może zaadaptować konfigurację maszyny wirtualnej do swoich potrzeb.

Komponent **Acronis Backup & Recovery 10 Agent dla systemu Windows** umożliwia odzyskanie kopii zapasowej dysku (woluminu) na nową maszynę wirtualną jednego z następujących typów: VMware Workstation, Microsoft Virtual PC, Parallels Workstation, Citrix XenServer Open Virtual Appliance (OVA) lub Red Hat KVM.

Program umieści pliki nowej maszyny wirtualnej w wybranym folderze. Maszynę można uruchomić przy użyciu odpowiedniego oprogramowania do wirtualizacji lub przygotować pliki maszyny do dalszego użycia. Urządzenie wirtualne Citrix XenServer Open Virtual Appliance (OVA) można zaimportować na serwer XenServer przy użyciu narzędzia Citrix XenCenter. Stację roboczą VMware można przekonwertować na otwarty format wirtualizacji (OVF) przy użyciu narzędzia VMware OVF.

Komponent **Acronis Backup & Recovery 10 Agent dla Hyper-V** lub **Agent dla ESX/ESXi** umożliwia odzyskanie kopii zapasowej dysku (woluminu) na nową maszynę wirtualną na odpowiednim serwerze wirtualizacji.

Wskazówka. *Maszyna wirtualna Microsoft Virtual PC nie obsługuje dysków większych niż 127 GB. Firma Acronis umożliwia tworzenie maszyn wirtualnych Virtual PC o większych dyskach, dlatego możesz podłączać dyski do maszyny wirtualnej Microsoft Hyper-V.*

Aby przekonwertować kopię zapasową dysku na maszynę wirtualną:

1. Połącz konsolę z komputerem, na którym jest zainstalowany agent dla systemu Windows, agent dla Hyper-V lub agent dla ESX/ESXi.
2. Wykonaj jedną z następujących czynności:
   - Kliknij **Odzyskaj**, aby otworzyć stronę **Odzyskaj dane**. Rozpocznij tworzenie zadania odzyskiwania w sposób opisany w sekcji „Odzyskiwanie danych”. Wybierz archiwum, a następnie wybierz kopię zapasową dysku lub woluminu, którą chcesz przekonwertować.
   - Za pomocą panelu **Nawigacja** przejdź do skarbca, w którym znajduje się archiwum. Wybierz archiwum, a następnie wybierz kopię zapasową dysku lub woluminu, którą chcesz przekonwertować. Kliknij **Odzyskaj jako maszynę wirtualną**. Pojawi się strona **Odzyskaj dane** ze wstępnie wybraną kopią zapasową.
3. W polu **Typ danych** wybierz **Dyski** lub **Woluminy**, w zależności od tego, co chcesz przekonwertować.
4. W polu **Zawartość** wybierz dyski do konwersji lub woluminy zawierające główne rekordy rozruchowe (MBR) odpowiednich dysków.
5. W polu **Odzyskaj do** wybierz **Nowa maszyna wirtualna**.
6. W polu **Serwer maszyny wirtualnej** wybierz typ nowej maszyny wirtualnej, którą chcesz utworzyć, *lub* serwer wirtualizacji, na którym chcesz ją utworzyć.
7. W polu **Nazwa maszyny wirtualnej** wprowadź nazwę nowej maszyny wirtualnej.
8. [Opcjonalnie] Sprawdź **Ustawienia maszyn wirtualnych (s. 259)** i w razie potrzeby wprowadź zmiany Można tutaj zmienić ścieżkę do nowej maszyny wirtualnej.

   W jednym folderze nie można utworzyć maszyn tego samego typu o takiej samej nazwie. W przypadku wystąpienia komunikatu o błędzie spowodowanego przez identyczne nazwy, należy zmienić nazwę maszyny wirtualnej lub jej ścieżkę.
9. Wybierz dysk docelowy dla każdego dysku źródłowego lub woluminu źródłowego i głównego rekordu startowego.

   W przypadku maszyny typu Microsoft Virtual PC dysk lub wolumin zawierający program ładujący systemu operacyjnego musi być odzyskany na dysk twardy 1. W przeciwnym razie nie będzie można uruchomić systemu operacyjnego. Tego błędu nie można naprawić przez zmianę kolejności urządzeń startowych w systemie BIOS, ponieważ maszyna typu Virtual PC ignoruje te ustawienia.
10. W polu **Czas odzyskiwania** określ czas rozpoczęcia zadania odzyskiwania.
11. [Opcjonalnie] Sprawdź **Opcje odzyskiwania** i w razie potrzeby zmień ustawienia domyślne. Wybierając **Opcje odzyskiwania > Zarządzanie zasilaniem maszyn wirtualnych**, możesz określić, czy po zakończeniu odzyskiwania chcesz automatycznie uruchomić nową maszynę wirtualną. Ta opcja jest dostępna tylko wtedy, gdy nowa maszyna wirtualna jest utworzona na serwerze wirtualizacji.
12. Kliknij **OK**. Jeśli zaplanujesz zadanie odzyskiwania w przyszłości, określ poświadczenia, z jakimi zostanie wykonane.

Program wyświetli widok **Plany i zadania tworzenia kopii zapasowych**, w którym można sprawdzić stan i postęp zadania odzyskiwania.

Operacje po konwersji

Wynikowy komputer zawsze ma interfejs dysku SCSI i podstawowe woluminy MBR. Jeśli komputer korzysta z niestandardowego programu ładującego, może wystąpić konieczność skonfigurowania tego programu, aby wskazać nowe urządzenia, i jego ponownej aktywacji. Konfigurację programu GRUB opisano w sekcji „Jak ponownie aktywować program GRUB i zmienić jego konfigurację (s. 267)".

Wskazówka. *Aby zachować woluminy logiczne (LVM) na komputerze z systemem Linux, warto rozważyć inną metodę konwersji. Utwórz nową maszynę wirtualną, uruchom ją za pomocą nośnika startowego i przeprowadź operację odzyskiwania w taki sam sposób, jak na komputerze fizycznym. Strukturę LVM można utworzyć ponownie w sposób automatyczny (s. 304) podczas odzyskiwania, jeśli została zapisana (s. 52) w kopii zapasowej.*

6.3.11 Rozwiązywanie problemów z funkcjami rozruchowymi dysku

Jeśli podczas tworzenia kopii zapasowej można uruchomić system, użytkownik oczekuje, że będzie tak również po odzyskaniu. Jednak informacje zapisywane i używane przez system operacyjny w celu uruchamiania mogą być przestarzałe po odzyskaniu, zwłaszcza po zmianie rozmiarów woluminów, lokalizacji lub dysków docelowych. Program Acronis Backup & Recovery 10 automatycznie aktualizuje moduły ładujące systemu Windows po odzyskaniu. Można również naprawić inne moduły ładujące, ale występują sytuacje, w których trzeba je ponownie aktywować. Zwłaszcza w przypadku odzyskiwania woluminów systemu Linux konieczne jest czasem zastosowanie poprawek w celu uwzględnienia zmian związanych z uruchamianiem, aby poprawnie uruchomić i załadować system Linux.

Poniżej przedstawiono podsumowanie typowych sytuacji wymagających wykonania dodatkowych czynności przez użytkownika.

Dlaczego odzyskany system operacyjny może być niemożliwy do uruchomienia

- **System BIOS komputera jest skonfigurowany do uruchamiania z innego dysku.**

  Rozwiązanie: Skonfiguruj system BIOS w celu uruchamiania z dysku twardego, na którym znajduje się system operacyjny.

- **System został odzyskany na innym sprzęcie, który jest niekompatybilny z większością najważniejszych sterowników zawartych w kopii zapasowej**

  Rozwiązanie dla systemu Windows: Odzyskaj wolumin ponownie. Podczas konfigurowania odzyskiwania wybierz opcję użycia funkcji Acronis Universal Restore i określ odpowiednie lokalizacje HAL i sterowniki pamięci masowej.

- **System Windows został odzyskany na wolumin dynamiczny, który nie może być startowy**

  Rozwiązanie: Odzyskaj system Windows na wolumin zwykły, prosty lub lustrzany.

- **Wolumin systemowy został odzyskany na dysk nie zawierający głównego rekordu rozruchowego (MBR)**

  Podczas konfigurowania odzyskiwania woluminu systemowego na dysk, który nie zawiera głównego rekordu rozruchowego, program wyświetla pytanie, czy wraz z woluminem systemowym ma odzyskać główny rekord rozruchowy. Opcję, w której rekord nie jest odzyskiwany należy wybrać tylko wtedy, gdy odzyskany system nie będzie uruchamiany.

  Rozwiązanie: Odzyskaj wolumin ponownie wraz z głównym rekordem rozruchowym odpowiedniego dysku.

- **System używa programu Acronis OS Selector**

  Ponieważ podczas odzyskiwania systemu można zmienić główny rekord rozruchowy (MBR), program Acronis OS Selector, który używa tego rekordu może przestać działać. Jeśli to nastąpi, aktywuj ponownie program Acronis OS Selector w następujący sposób.

  Rozwiązanie: Uruchom komputer przy użyciu nośnika startowego programu Acronis Disk Director i wybierz z menu **Narzędzia -> Activate OS Selector**.

- **System używa modułu GRand Unified Bootloader (GRUB) i został odzyskany z normalnej kopii zapasowej (nie z kopii nieprzetworzonej, czyli utworzonej „sektor po sektorze")**

  Pewna część modułu ładującego GRUB znajduje się w pierwszych kilku sektorach dysku lub woluminu. Pozostała część znajduje się w systemie plików na jednym z woluminów. Możliwość uruchamiania systemu można przywrócić automatycznie tylko wówczas, gdy moduł GRUB znajduje się w pierwszych kilku sektorach dysku oraz w systemie plików, do którego możliwy jest bezpośredni dostęp. W przeciwnym razie należy ręcznie aktywować ponownie moduł ładujący.

  Rozwiązanie: Aktywuj ponownie moduł ładujący. Konieczne może być również naprawienie pliku konfiguracyjnego.

- **System używa modułu Linux Loader (LILO) i został odzyskany z normalnej kopii zapasowej (nie z kopii nieprzetworzonej, czyli utworzonej „sektor po sektorze")**

  Moduł LILO zawiera wiele odwołań do bezwzględnych numerów sektorów i dlatego nie można go automatycznie naprawić z wyjątkiem sytuacji, w której program odzyska wszystkie dane do sektorów o takich samych numerach bezwzględnych, jak na dysku źródłowym.

  Rozwiązanie: Aktywuj ponownie moduł ładujący. Konieczne może być również naprawienie pliku konfiguracyjnego z przyczyn opisanych w poprzednim akapicie.

- **Moduł ładujący system wskazuje na nieprawidłowy wolumin**

  Może to nastąpić, gdy wolumin systemowy lub startowy nie zostanie odzyskany w oryginalnych lokalizacjach.

  Rozwiązanie:

  Zmodyfikowanie plików boot.ini lub boot\bcd umożliwia naprawienie tych problemów w przypadku modułów ładujących w systemie Windows. Program Acronis Backup & Recovery 10 robi to automatycznie i te problemy nie powinny występować.

  Dla modułów GRUB i LILO konieczne jest poprawienie plików konfiguracyjnych GRUB. Jeśli numer partycji głównej systemu Linux uległ zmianie, zaleca się również zmianę pliku /etc/fstab tak, aby zapewnić prawidłowy dostęp do woluminu SWAP.

- **System Linux odzyskany z kopii zapasowej woluminu LVM na podstawowy dysk z głównym rekordem rozruchowym**

  Takiego systemu nie można uruchomić, ponieważ jego jądro próbuje zamontować podstawowy system plików w woluminie LVM.

  Rozwiązanie: Zmień konfigurację modułu ładującego i plik /etc/fstab tak, aby nie używać woluminu LVM, a następnie aktywuj ponownie moduł ładujący.

Jak ponownie aktywować program GRUB i zmienić jego konfigurację

Zwykle odpowiednia procedura znajduje się w podręczniku programu ładującego. W witrynie internetowej firmy Acronis znajduje się również odpowiedni artykuł bazy wiedzy.

Poniżej przedstawiono przykład ponownej aktywacji programu GRUB w przypadku odzyskiwania dysku (woluminu) systemowego na identyczny sprzęt.

1. Uruchom system Linux lub uruchom komputer z nośnika startowego, a następnie naciśnij klawisze CTRL+ALT+F2.

2. Zamontuj odzyskiwany system:

```
mkdir /mnt/system/
mount -t ext3 /dev/sda2 /mnt/system/ # partycja główna
mount -t ext3 /dev/sda1 /mnt/system/boot/ # partycja startowa
```

3. Zamontuj systemy plików **proc** i **dev** w odzyskiwanym systemie:

```
mount -t proc none /mnt/system/proc/
mount -o bind /dev/ /mnt/system/dev/
```

4. Zapisz kopię pliku menu GRUB, uruchamiając jedno z następujących poleceń:

```
cp /mnt/system/boot/grub/menu.lst /mnt/system/boot/grub/menu.lst.backup
```

lub

```
cp /mnt/system/boot/grub/grub.conf /mnt/system/boot/grub/grub.conf.backup
```

5. Zmodyfikuj plik **/mnt/system/boot/grub/menu.lst** (dystrybucje Debian, Ubuntu i SUSE Linux) lub plik **/mnt/system/boot/grub/grub.conf** (dystrybucje Fedora i Red Hat Enterprise Linux) — na przykład w następujący sposób:

```
vi /mnt/system/boot/grub/menu.lst
```

6. W pliku **menu.lst** (lub odpowiednio **grub.conf**) znajdź element menu odpowiadający odzyskiwanemu systemowi. Elementy takiego menu mają następującą postać:

```
title Red Hat Enterprise Linux Server (2,6.24,4)
      root (hd0,0)
      kernel /vmlinuz-2,6.24,4 ro root=/dev/sda2 rhgb quiet
      initrd /initrd-2,6.24,4.img
```

W wierszach rozpoczynających się od **title**, **root**, **kernel** i **initrd** określone są odpowiednio:

- Tytuł elementu menu.
- Urządzenie, na którym znajduje się jądro systemu Linux — zwykle jest to partycja startowa lub partycja główna, taka jak **root (hd0,0)** w niniejszym przykładzie.
- Ścieżka do jądra na tym urządzeniu i partycja główna. W tym przykładzie ścieżka to **/vmlinuz-2.6.24.4**, a partycja główna — **/dev/sda2**. Partycję główną można określić, podając etykietę (na przykład **root=LABEL=/**), identyfikator (w postaci **root=UUID=***jakiś_uuid*) lub nazwę urządzenia (na przykład **root=/dev/sda2**).
- Ścieżka do usługi **initrd** na tym urządzeniu.

7. Zmodyfikuj plik **/mnt/system/etc/fstab**, aby poprawić nazwy wszelkich urządzeń, które zmieniły się w wyniku odzyskiwania.
8. Uruchom powłokę GRUB przy użyciu jednego z następujących poleceń:

```
chroot /mnt/system/ /sbin/grub
```

lub

```
chroot /mnt/system/ /usr/sbin/grub
```

9. Określ dysk, na którym znajduje się program GRUB. Zwykle jest to partycja startowa lub główna:

```
root (hd0,0)
```

10. Zainstaluj program GRUB. Aby na przykład zainstalować go w głównym rekordzie rozruchowym (MBR) pierwszego dysku, uruchom następujące polecenie:

```
setup (hd0)
```

11. Zamknij powłokę GRUB:

```
quit
```


12. Odmontuj zamontowane systemy plików i ponownie uruchom komputer:

```
umount /mnt/system/dev/
umount /mnt/system/proc/
umount /mnt/system/boot/
umount /mnt/system/
reboot
```

13. Ponownie skonfiguruj program ładujący, korzystając z narzędzi i dokumentacji używanej dystrybucji systemu Linux. Na przykład w dystrybucjach Debian i Ubuntu może być konieczna edycja ujętych w komentarz wierszy w pliku **/boot/grub/menu.lst**, a następnie uruchomienie skryptu **update-grub**. W przeciwnym razie zmiany mogą nie zostać uwzględnione.

Moduły ładujące w systemie Windows

Windows NT/2000/XP/2003

Pewna część modułu ładującego znajduje się w sektorze startowym partycji, a pozostała część w plikach ntldr, boot.ini, ntdetect.com, ntbootdd.sys. Plik boot.ini jest plikiem tekstowym zawierającym konfigurację modułu ładującego. Przykład:

```
[boot loader]
timeout=30
default=multi(0)disk(0)rdisk(0)partition(1)\WINDOWS
[operating systems]
multi(0)disk(0)rdisk(0)partition(1)\WINDOWS="Microsoft Windows XP Professional"
/noexecute=optin /fastdetect
```

Windows Vista/2008

Pewna część modułu ładującego znajduje się w sektorze startowym partycji, a pozostała część w plikach bootmgr, boot\bcd. Po uruchomieniu systemu Windows plik boot\bcd jest montowany w kluczu rejestru HKLM \BCD00000000.

6.3.12 Składanie urządzeń MD do odzyskiwania (Linux)

W systemie Linux przed odzyskaniem danych z kopii zapasowej dysku na istniejące urządzenie MD (zwane również programowym urządzeniem RAID systemu Linux) należy się upewnić, że **urządzenie zostało złożone**.

Jeśli tak nie jest, należy je złożyć przy użyciu narzędzia **mdadm**. Oto dwa przykłady:

Przykład 1. Następujące polecenie umożliwia złożenie urządzenia /dev/md0 z woluminów /dev/sdb1 i /dev/sdc1:

```
mdadm --assemble /dev/md0 -ayes /dev/sdb1 /sdc1
```

Przykład 2. Następujące polecenie umożliwia złożenie urządzenia /dev/md0 z dysków /dev/sdb i /dev/sdc:

```
mdadm --assemble /dev/md0 -ayes /dev/sdb /dev/sdc
```

Jeśli odzyskanie wymaga ponownego uruchomienia komputera (zwykle wówczas, gdy odzyskiwane woluminy obejmują partycję startową), należy postępować według następujących wskazówek:

- Jeśli wszystkie części urządzenia MD to woluminy (typowy przypadek, tak jak w pierwszym przykładzie), upewnij się, że typ każdego woluminu — nazywany typem partycji lub identyfikatorem systemu — to **Linux raid automount**. Kod szesnastkowy takiego typu partycji to 0xFD. Gwarantuje to automatyczne złożenie urządzenia po ponownym uruchomieniu komputera.

Aby wyświetlić lub zmienić typ partycji, użyj narzędzia do partycjonowania dysków, na przykład **fdisk**.

- W przeciwnym razie (takim, jak w drugim przykładzie) odzyskaj urządzenie z nośnika startowego. Nie jest wówczas wymagane ponowne uruchomienie komputera. Na nośniku startowym może być konieczne ręczne utworzenie urządzenia MD zgodnie z opisem w sekcji Odzyskiwanie urządzeń MD i woluminów logicznych (s. 304).

6.3.13 Odzyskiwanie dużej liczby plików z kopii zapasowej na poziomie plików

Dotyczy systemu: Microsoft Windows Server 2003

Podczas jednoczesnego odzyskiwania z kopii zapasowej na poziomie plików dużej liczby plików (setek tysięcy lub milionów) może wystąpić następujący problem:

- Proces odzyskiwania zakończy się niepowodzeniem i program wyświetli komunikat „Wystąpił błąd podczas odczytywania pliku”.
- Nie wszystkie pliki zostaną odzyskane.

Prawdopodobną przyczyną tego problemu jest niewystarczająca ilość pamięci przydzielonej dla procesu odzyskiwania przez menedżera pamięci podręcznej systemu. W tej sytuacji można obejść ten problem lub zmodyfikować rejestr w celu zwiększenia ilości przydzielonej pamięci w sposób opisany poniżej.

Aby rozwiązać problem, wykonaj jedną z następujących czynności:

- Odzyskaj pliki w kilku grupach. Jeśli na przykład problem występuje podczas odzyskiwania 1 miliona plików, spróbuj odzyskać pierwsze 500 000 plików, a następnie pozostałe 500 000.
- Zmodyfikuj rejestr w następujący sposób:

  Uwaga: *Ta procedura wymaga ponownego uruchomienia komputera. Podczas modyfikowania rejestru należy zachować standardowe środki ostrożności.*

  1. W Edytorze rejestru otwórz następujący podklucz:

  ```
  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management
  ```

  2. Dodaj do podklucza wpis **PoolUsageMaximum**:
     - Typ wpisu: **Wartość DWORD**
     - System: **Dziesiętny**
     - Wartość: **40**
  3. Dodaj do podklucza wpis **PagedPoolSize**:
     - Typ wpisu: **Wartość DWORD**
     - System: **Szesnastkowy**
     - Wartość: **FFFFFFFF**
  4. Zamknij Edytor rejestru i uruchom ponownie komputer.

  Jeśli nie spowoduje to rozwiązania problemu, aby rozwiązać problem lub uzyskać więcej informacji na temat dodawania ustawień rejestru, zapoznaj się z odpowiednim artykułem pomocy i wsparcia firmy Microsoft.

Wskazówka: *Ogólnie rzecz biorąc, jeśli wolumin zawiera dużą liczbę plików, należy rozważyć utworzenie kopii zapasowej na poziomie dysków, a nie na poziomie plików. W takim przypadku można odzyskać cały wolumin, a także zapisane na nim poszczególne pliki.*

6.3.14 Odzyskiwanie węzła magazynowania

Oprócz tworzenia kopii zapasowych danych w skarbcach centralnych zarządzanych przy użyciu węzła Acronis Backup & Recovery 10 Storage Node można również tworzyć kopie zapasowe dysków komputera, na którym jest zainstalowany ten węzeł.

W tej sekcji opisano sposób odzyskiwania węzła magazynowania zarejestrowanego na serwerze zarządzania w przypadku, gdy znajdują się one na różnych komputerach (jeśli węzeł i serwer są zainstalowane na tym samym komputerze, wystarczy odzyskać ten komputer).

Rozważmy następujący scenariusz:

- Serwer zarządzania znajduje się na jednym komputerze, a węzeł magazynowania na drugim.
- Węzeł magazynowania jest zarejestrowany na serwerze zarządzania.
- Odzyskujesz wcześniej utworzoną kopię zapasową komputera zawierającego węzeł magazynowania. Kopię odzyskujesz na ten sam lub inny komputer.

Przed użyciem odzyskanego węzła magazynowania wykonaj następujące czynności:

- Jeśli węzeł magazynowania został odzyskany na ten sam komputer, a między chwilą utworzenia kopii zapasowej i jej odzyskaniem nie dodano ani nie usunięto centralnych skarbców zarządzanych przez ten węzeł, nie wykonuj żadnych czynności.
- W przeciwnym przypadku wykonaj następujące czynności:
  1. Połącz się z serwerem zarządzania i usuń z niego węzeł magazynowania.

     Uwaga: *Z serwera zarządzania program usunie również wszystkie skarbce zarządzane przez węzeł magazynowania. Archiwa nie zostaną utracone.*

  2. Dodaj ponownie węzeł magazynowania do serwera zarządzania, określając komputer, na którym jest zainstalowany odzyskany węzeł magazynowania.
  3. Utwórz ponownie niezbędne skarbce zarządzane.

6.4 Sprawdzanie poprawności skarbców, archiwów i kopii zapasowych

Operacja sprawdzania poprawności polega na sprawdzeniu, czy można odzyskać dane z kopii zapasowej.

Sprawdzanie poprawności kopii zapasowej plików symuluje odzyskiwanie wszystkich plików z kopii zapasowej do tymczasowego miejsca docelowego. Sprawdzanie poprawności kopii zapasowej dysku lub woluminu polega na obliczeniu sumy kontrolnej wszystkich bloków danych zapisanych w kopii zapasowej. Obie procedury intensywnie korzystają z zasobów.

Sprawdzenie poprawności archiwum oznacza sprawdzenie wszystkich kopii zapasowych tego archiwum. Sprawdzenie poprawności skarbca (lub lokalizacji) oznacza sprawdzenie wszystkich archiwów przechowywanych w tym skarbcu (lokalizacji).

Jeśli operacja sprawdzania poprawności zakończy się powodzeniem, istnieje wysokie prawdopodobieństwo pomyślnego odzyskania danych. Nie są jednak sprawdzane wszystkie czynniki, które mają wpływ na proces odzyskiwania. Po utworzeniu kopii zapasowej systemu operacyjnego gwarancję pomyślnego odzyskania danych w przyszłości można uzyskać jedynie na podstawie testu, który polega na odzyskaniu danych z nośnika startowego na zapasowy dysk twardy. Upewnij się

przynajmniej, że można z powodzeniem sprawdzić poprawność kopii zapasowej przy użyciu nośnika startowego.

Różne metody tworzenia zadania sprawdzania poprawności

Korzystanie ze strony sprawdzania poprawności to najpopularniejszy sposób tworzenia zadania sprawdzania poprawności. Można na niej od razu sprawdzić poprawność lub ustalić harmonogram sprawdzania poprawności dowolnej kopii zapasowej, archiwum lub lokalizacji, które są dostępne w ramach posiadanych uprawnień.

Sprawdzanie poprawności archiwum lub najnowszej kopii zapasowej w archiwum można zaplanować jako część planu tworzenia kopii zapasowych. Aby uzyskać więcej informacji na ten temat, zobacz sekcję Tworzenie planu tworzenia kopii zapasowych (s. 219).

Dostęp do strony **Sprawdzanie poprawności** można uzyskać w widoku **Skarbce** (s. 144). Kliknij prawym przyciskiem myszy obiekt (archiwum, kopię zapasową lub skarbiec) do sprawdzenia poprawności i wybierz polecenie **Sprawdź poprawność** w menu kontekstowym. Zostanie otwarta strona Sprawdzanie poprawności ze wstępnie wybranym obiektem jako źródłem. Wystarczy jedynie wybrać czas sprawdzania poprawności oraz (opcjonalnie) wprowadzić nazwę zadania.

Aby utworzyć zadanie sprawdzania poprawności, wykonaj poniższe kroki

Ogólne

Nazwa zadania

[Opcjonalnie] Wprowadź unikatową nazwę zadania sprawdzania poprawności. Dobrze dobrana nazwa pozwala na szybką identyfikację zadania pośród innych zadań.

Poświadczenia (s. 273)

[Opcjonalnie] Zadanie będzie wykonywane w imieniu użytkownika, który je utworzył. W razie potrzeby można zmienić poświadczenia zadania. Aby uzyskać dostęp do tej opcji, zaznacz pole wyboru **Widok zaawansowany**.

Elementy do sprawdzenia poprawności

Sprawdź poprawność

Wybierz obiekt do sprawdzenia poprawności:

Archiwum (s. 273) — w tym miejscu należy określić archiwum.

Kopia zapasowa (s. 274) — najpierw określ archiwum, a następnie wybierz żądaną kopię zapasową w tym archiwum.

Skarbiec (s. 274) — wybierz skarbiec (lub inną lokalizację) oraz archiwa do sprawdzenia poprawności.

Poświadczenia dostępu (s. 275)

[Opcjonalnie] Jeśli konto zadania nie posiada wystarczających uprawnień dostępu do źródła, podaj poświadczenia dostępu. Aby uzyskać dostęp do tej opcji, zaznacz pole wyboru **Widok zaawansowany**.

Czas sprawdzania poprawności

Sprawdź poprawność (s. 275)

Określ czas i częstotliwość sprawdzania poprawności.

Po skonfigurowaniu wszystkich wymaganych ustawień kliknij **OK**, aby utworzyć zadanie sprawdzania poprawności.

6.4.1 Poświadczenia zadania

Określ poświadczenia konta, na którym zadanie będzie uruchamiane.

Aby określić poświadczenia

1. Wybierz jedną z następujących opcji:
   - **Użyj poświadczeń bieżącego użytkownika**

     Zadanie będzie uruchamiane przy użyciu poświadczeń, z którymi zalogował się użytkownik rozpoczynający zadania. Jeśli zadanie ma zostać uruchomione według harmonogramu, w momencie zakończenia tworzenia zadania użytkownik zostanie poproszony o aktualne hasło użytkownika.
   - **Użyj następujących poświadczeń**

     Zadanie będzie zawsze uruchamiane przy użyciu poświadczeń określonych przez użytkownika, niezależnie od tego, czy zadanie będzie uruchamiane ręcznie, czy wykonywane według harmonogramu.

     Określ:
     - **Nazwa użytkownika**. Wprowadzając nazwę konta użytkownika usługi Active Directory, należy określić również nazwę domeny (DOMENA\Nazwa_użytkownika lub Nazwa_użytkownika@domena).
     - **Hasło**. Hasło dla konta.
2. Kliknij **OK**.

Więcej informacji na temat używania poświadczeń w programie Acronis Backup & Recovery 10 można znaleźć w sekcji Właściciele i poświadczenia (s. 35).

Aby dowiedzieć się więcej na temat operacji dostępnych w zależności od uprawnień użytkownika, zobacz sekcję Uprawnienia użytkownika na komputerze zarządzanym (s. 34).

6.4.2 Wybór archiwum

Wybieranie archiwum

1. Wprowadź pełną ścieżkę do lokalizacji w polu **Ścieżka** lub wybierz odpowiedni folder w drzewie folderów.
   - Jeśli archiwum znajduje się w magazynie Acronis Online Backup Storage, kliknij **Zaloguj** i określ poświadczenia logowania do magazynu online. Następnie rozwiń grupę **Magazyn kopii zapasowych online** i wybierz konto.

   W przypadku kopii zapasowych zapisanych w magazynie Acronis Online Backup Storage nie są obsługiwane operacje eksportowania i montowania.
   - Jeśli archiwum znajduje się w skarbcu centralnym, rozwiń grupę **Centralne** i kliknij skarbiec.
   - Jeśli archiwum znajduje się w skarbcu osobistym, rozwiń grupę **Osobiste** i kliknij skarbiec.
   - Jeśli archiwum znajduje się w folderze lokalnym na komputerze, rozwiń grupę **Foldery lokalne** i kliknij odpowiedni folder.

   Jeśli archiwum znajduje się na nośniku wymiennym, na przykład na płycie DVD, najpierw włóż ostatnią płytę DVD, a następnie zgodnie z wyświetlanymi monitami wkładaj kolejno pozostałe płyty, zaczynając od pierwszej.

- Jeśli archiwum znajduje się w udziale sieciowym, rozwiń grupę **Foldery sieciowe**, wybierz żądany komputer sieciowy, a następnie kliknij folder udostępniony. Jeśli udział sieciowy wymaga poświadczeń dostępu, program wyświetli odpowiedni monit.

Uwaga dla użytkowników systemu Linux: *Aby określić udział sieciowy CIFS (Common Internet File System) zamontowany w punkcie montowania, takim jak /mnt/share, należy wybrać ten punkt montowania, a nie sam udział sieciowy.*

- Jeśli archiwum znajduje się na serwerze **FTP** lub **SFTP**, w polu **Ścieżka** wpisz nazwę lub adres serwera w następujący sposób:

  ftp://serwer_ftp:numer_portu lub sftp://serwer_sftp:numer_portu

  Jeśli nie określisz numeru portu, dla serwera FTP zostanie użyty port 21, a dla SFTP — 22.

  Po wprowadzeniu poświadczeń dostępu zostaną udostępnione foldery na serwerze. Kliknij odpowiedni folder.

  Dostęp do serwera można uzyskać jako użytkownik anonimowy, o ile serwer zezwala na taki dostęp. W tym celu nie trzeba wprowadzać poświadczeń, lecz należy kliknąć opcję **Użyj dostępu anonimowego**.

Jak wynika z oryginalnej specyfikacji protokołu FTP, poświadczenia wymagane do uzyskania dostępu do serwerów FTP są przesyłane w sieci jako otwarty tekst. Oznacza to, że nazwę użytkownika i hasło można przejąć przy użyciu programu do przechwytywania pakietów.

- Jeśli archiwum znajduje się na podłączonym lokalnie urządzeniu taśmowym, rozwiń grupę **Napędy taśmowe** i kliknij odpowiednie urządzenie.

W przypadku pracy na komputerze uruchamianym z nośnika startowego:

- Aby uzyskać dostęp do skarbca zarządzanego, w polu **Ścieżka** wpisz następujący ciąg:

  bsp://adres_węzła/nazwa_skarbca/

- Aby uzyskać dostęp do niezarządzanego skarbca centralnego, wpisz pełną ścieżkę do folderu skarbca.

2. Wybierz archiwum w tabeli po prawej stronie drzewa. Tabela przedstawia nazwy archiwów znajdujących się w każdym wybranym przez użytkownika skarbcu lub folderze.

   Gdy przeglądasz zawartość lokalizacji, inni użytkownicy lub sam program mogą dodać, usunąć lub zmodyfikować archiwa. Przycisk **Odśwież** pozwala odświeżyć listę archiwów.
3. Kliknij **OK**.

6.4.3 Wybór kopii zapasowej

Aby określić kopię zapasową w celu sprawdzenia poprawności

1. W górnym panelu wybierz kopię zapasową według daty/godziny jej utworzenia.

   W dolnej części okna program wyświetli zawartość wybranej kopii zapasowej, co ułatwia znalezienie właściwej kopii.
2. Kliknij **OK**.

6.4.4 Wybór lokalizacji

Aby wybrać lokalizację

Wprowadź pełną ścieżkę do lokalizacji w polu **Ścieżka**, lub wybierz odpowiednią lokalizację w **drzewie folderów**.

- Aby wybrać skarbiec centralny, rozwiń grupę **Centralne** i kliknij odpowiedni skarbiec.
- Aby wybrać skarbiec osobisty, rozwiń grupę **Osobiste** i kliknij odpowiedni skarbiec.

- Aby wybrać folder lokalny (płytę CD/DVD lub podłączone lokalnie urządzenie taśmowe), rozwiń grupę **Foldery lokalne** i kliknij wymagany folder.
- Aby wybrać udział sieciowy, rozwiń grupę **Foldery sieciowe**, wybierz komputer w sieci, a następnie kliknij udostępniony folder. Jeśli udział sieciowy wymaga poświadczeń dostępu, program wyświetli odpowiedni monit.
- Aby wybrać folder **FTP** lub **SFTP**, rozwiń odpowiednią grupę i kliknij folder na serwerze.

Jak wynika z oryginalnej specyfikacji protokołu FTP, poświadczenia wymagane do uzyskania dostępu do serwerów FTP są przesyłane w sieci jako otwarty tekst. Oznacza to, że nazwę użytkownika i hasło można przejąć przy użyciu programu do przechwytywania pakietów.

Używanie tabeli archiwów

Aby ułatwić wybranie właściwej lokalizacji, w tabeli przedstawione są nazwy archiwów znajdujących się we wszystkich wybranych lokalizacjach. Gdy przeglądasz zawartość lokalizacji, inni użytkownicy lub sam program mogą dodać, usunąć lub zmodyfikować archiwa. Przycisk **Odśwież** pozwala odświeżyć listę archiwów.

6.4.5 Poświadczenia dostępu dla źródła

Określ poświadczenia wymagane do uzyskania dostępu do lokalizacji, w której znajduje się archiwum kopii zapasowej.

Aby określić poświadczenia

1. Wybierz jedną z następujących opcji:
   - **Użyj poświadczeń zadania**

     Program użyje poświadczeń konta zadania określonych w sekcji Ogólne w celu dostępu do lokalizacji.
   - **Użyj następujących poświadczeń**

     Program uzyska dostęp do lokalizacji przy użyciu określonych poświadczeń. Tej opcji należy użyć, gdy konto zadania nie ma uprawnień dostępu do lokalizacji. Konieczne może być podanie specjalnych poświadczeń dla udziału sieciowego lub skarbca węzła magazynowania.

     Określ:
     - **Nazwa użytkownika**. Wprowadzając nazwę konta użytkownika usługi Active Directory, należy określić również nazwę domeny (DOMENA\Nazwa_użytkownika lub Nazwa_użytkownika@domena).
     - **Hasło**. Hasło dla konta.
2. Kliknij **OK**.

Jak wynika z oryginalnej specyfikacji protokołu FTP, poświadczenia wymagane do uzyskania dostępu do serwerów FTP są przesyłane w sieci jako otwarty tekst. Oznacza to, że nazwę użytkownika i hasło można przejąć przy użyciu programu do przechwytywania pakietów.

6.4.6 Czas sprawdzania poprawności

Ponieważ operacja sprawdzania poprawności wymaga użycia dużej ilości zasobów, najlepiej zaplanować jej wykonanie wtedy, gdy obciążenie zarządzanego komputera jest najmniejsze. Jednak, aby dowiedzieć się jak najszybciej, czy dane nie są uszkodzone i czy można je pomyślnie odzyskać, należy rozpocząć sprawdzanie poprawności natychmiast po utworzeniu zadania.

Wybierz jedną z następujących opcji:

- **Teraz** — aby rozpocząć zadanie sprawdzania poprawności natychmiast po jego utworzeniu, to znaczy po kliknięciu OK na stronie Sprawdzanie poprawności.
- **Później** — aby rozpocząć zadanie sprawdzania poprawności w określonym dniu i o określonej godzinie.

  Określ odpowiednie parametry:

  - **Data i godzina** — data i godzina rozpoczęcia zadania.
  - **Zadanie zostanie uruchomione ręcznie (nie planuj zadania)** — zaznacz to pole wyboru, jeśli chcesz uruchomić zadanie ręcznie w późniejszym terminie.
- **Według harmonogramu** — aby zaplanować uruchomienie zadania. Więcej informacji na temat konfigurowania parametrów harmonogramu można znaleźć w sekcji Planowanie (s. 185).

6.5 Montowanie obrazu

Zamontowanie woluminów z kopii zapasowej (obrazu) dysku umożliwia dostęp do woluminów tak, jakby były one dyskami fizycznymi. Podczas jednej operacji montowania można zamontować kilka woluminów zawartych w jednej kopii zapasowej. Operacja montowania jest dostępna, gdy konsola jest połączona z zarządzanym komputerem, na którym działa system Windows lub Linux.

Zamontowanie woluminów w trybie do odczytu i zapisu umożliwia modyfikowanie zawartości kopii zapasowej, czyli zapisywanie, przenoszenie, tworzenie, usuwanie plików lub folderów i uruchamianie programów składających się z jednego pliku.

Ograniczenie: *Zamontowanie kopii zapasowych woluminów zapisanych w węźle magazynowania Acronis Backup & Recovery 10 Storage Node jest niemożliwe.*

Aby zamontować obraz, wykonaj następujące czynności.

Źródło

Archiwum (s. 277)

Określ ścieżkę do lokalizacji archiwum i wybierz archiwum zawierające kopie zapasowe dysków.

Kopia zapasowa (s. 278)

Wybierz kopię zapasową.

Poświadczenia dostępu (s. 278)

[Opcjonalnie] Podaj poświadczenia dla lokalizacji archiwum. Aby uzyskać dostęp do tej opcji, zaznacz pole wyboru **Widok zaawansowany**.

Ustawienia montowania

Woluminy (s. 278)

Wybierz woluminy, które chcesz zamontować i skonfiguruj ustawienia montowania dla każdego woluminu: przypisz literę lub wprowadź punkt montowania, wybierz tryb dostępu do odczytu i zapisu lub tylko do odczytu.

Po wykonaniu niezbędnych czynności kliknij **OK**, aby zamontować woluminy.

6.5.1 Wybór archiwum

Wybieranie archiwum

1. Wprowadź pełną ścieżkę do lokalizacji w polu **Ścieżka** lub wybierz odpowiedni folder w drzewie folderów.
   - Jeśli archiwum znajduje się w magazynie Acronis Online Backup Storage, kliknij **Zaloguj** i określ poświadczenia logowania do magazynu online. Następnie rozwiń grupę **Magazyn kopii zapasowych online** i wybierz konto.

   W przypadku kopii zapasowych zapisanych w magazynie Acronis Online Backup Storage nie są obsługiwane operacje eksportowania i montowania.

   - Jeśli archiwum znajduje się w skarbcu centralnym, rozwiń grupę **Centralne** i kliknij skarbiec.
   - Jeśli archiwum znajduje się w skarbcu osobistym, rozwiń grupę **Osobiste** i kliknij skarbiec.
   - Jeśli archiwum znajduje się w folderze lokalnym na komputerze, rozwiń grupę **Foldery lokalne** i kliknij odpowiedni folder.

   Jeśli archiwum znajduje się na nośniku wymiennym, na przykład na płycie DVD, najpierw włóż ostatnią płytę DVD, a następnie zgodnie z wyświetlanymi monitami wkładaj kolejno pozostałe płyty, zaczynając od pierwszej.

   - Jeśli archiwum znajduje się w udziale sieciowym, rozwiń grupę **Foldery sieciowe**, wybierz żądany komputer sieciowy, a następnie kliknij folder udostępniony. Jeśli udział sieciowy wymaga poświadczeń dostępu, program wyświetli odpowiedni monit.

   ***Uwaga dla użytkowników systemu Linux:** Aby określić udział sieciowy CIFS (Common Internet File System) zamontowany w punkcie montowania, takim jak /mnt/share, należy wybrać ten punkt montowania, a nie sam udział sieciowy.*

   - Jeśli archiwum znajduje się na serwerze **FTP** lub **SFTP**, w polu **Ścieżka** wpisz nazwę lub adres serwera w następujący sposób:

     ftp://serwer_ftp:numer_portu lub sftp://serwer_sftp:numer_portu

     Jeśli nie określisz numeru portu, dla serwera FTP zostanie użyty port 21, a dla SFTP — 22.

     Po wprowadzeniu poświadczeń dostępu zostaną udostępnione foldery na serwerze. Kliknij odpowiedni folder.

     Dostęp do serwera można uzyskać jako użytkownik anonimowy, o ile serwer zezwala na taki dostęp. W tym celu nie trzeba wprowadzać poświadczeń, lecz należy kliknąć opcję **Użyj dostępu anonimowego**.

   Jak wynika z oryginalnej specyfikacji protokołu FTP, poświadczenia wymagane do uzyskania dostępu do serwerów FTP są przesyłane w sieci jako otwarty tekst. Oznacza to, że nazwę użytkownika i hasło można przejąć przy użyciu programu do przechwytywania pakietów.

   - Jeśli archiwum znajduje się na podłączonym lokalnie urządzeniu taśmowym, rozwiń grupę **Napędy taśmowe** i kliknij odpowiednie urządzenie.

   W przypadku pracy na komputerze uruchamianym z nośnika startowego:

   - Aby uzyskać dostęp do skarbca zarządzanego, w polu **Ścieżka** wpisz następujący ciąg:

     bsp://adres_węzła/nazwa_skarbca/
   - Aby uzyskać dostęp do niezarządzanego skarbca centralnego, wpisz pełną ścieżkę do folderu skarbca.
2. Wybierz archiwum w tabeli po prawej stronie drzewa. Tabela przedstawia nazwy archiwów znajdujących się w każdym wybranym przez użytkownika skarbcu lub folderze.

Gdy przeglądasz zawartość lokalizacji, inni użytkownicy lub sam program mogą dodać, usunąć lub zmodyfikować archiwa. Przycisk **Odśwież** pozwala odświeżyć listę archiwów.

3. Kliknij **OK**.

6.5.2 Wybór kopii zapasowej

Aby wybrać kopię zapasową:

1. Wybierz jedną z kopii zapasowych według daty/godziny jej utworzenia.
2. Aby ułatwić wybranie właściwej kopii zapasowej, w tabeli poniżej przedstawione są woluminy znajdujące się w wybranej kopii zapasowej.

   Aby uzyskać informacje na temat woluminu, kliknij go prawym przyciskiem myszy, a następnie kliknij **Informacja**.
3. Kliknij **OK**.

6.5.3 Poświadczenia dostępu

Aby określić poświadczenia

1. Wybierz jedną z następujących opcji:
   - **Użyj poświadczeń bieżącego użytkownika**

     Program uzyska dostęp do lokalizacji przy użyciu poświadczeń bieżącego użytkownika.
   - **Użyj następujących poświadczeń**

     Program uzyska dostęp do lokalizacji przy użyciu określonych poświadczeń. Tej opcji należy użyć, gdy konto bieżącego użytkownika nie ma uprawnień dostępu do lokalizacji. Konieczne może być podanie specjalnych poświadczeń dla udziału sieciowego lub skarbca węzła magazynowania.

     Określ:
     - **Nazwa użytkownika**. Wprowadzając nazwę konta użytkownika usługi Active Directory, należy określić również nazwę domeny (DOMENA\Nazwa_użytkownika lub Nazwa_użytkownika@domena).
     - **Hasło**. Hasło dla konta.
2. Kliknij **OK**.

Jak wynika z oryginalnej specyfikacji protokołu FTP, poświadczenia wymagane do uzyskania dostępu do serwerów FTP są przesyłane w sieci jako otwarty tekst. Oznacza to, że nazwę użytkownika i hasło można przejąć przy użyciu programu do przechwytywania pakietów.

6.5.4 Wybór woluminu

Wybierz woluminy, które chcesz zamontować i skonfiguruj parametry montowania każdego z wybranych woluminów w następujący sposób:

1. Zaznacz pole wyboru obok wszystkich woluminów, które chcesz zamontować.
2. Kliknij wybrany wolumin, aby ustawić jego parametry montowania.
   - **Tryb dostępu** — wybierz tryb dostępu, w którym chcesz zamontować wolumin:
     - **Tylko do odczytu** — umożliwia przeglądanie i otwieranie plików w kopii zapasowej bez dokonywania żadnych zmian.
     - **Odczyt/zapis** — w tym trybie program może modyfikować zawartość kopii zapasowej i tworzy w tym celu przyrostową kopię zapasową, w której zapisuje zmiany.

- **Przypisz literę** (w systemie Windows) — Program Acronis Backup & Recovery 10 przypisze nieużywaną literę do montowanego woluminu. W razie konieczności można wybrać inną literę z listy rozwijanej.
- **Punkt zamontowania** (w systemie Linux) — określ katalog, w którym chcesz zamontować wolumin.

3. Jeśli do zamontowania wybrano kilka woluminów, kliknij każdy z nich, aby ustawić jego parametry montowania, co zostało opisane w poprzednim kroku.
4. Kliknij **OK**.

6.6 Zarządzanie zamontowanymi obrazami

Po zamontowaniu woluminu można przy użyciu menedżera plików przeglądać pliki i foldery zawarte w kopii zapasowej i kopiować wybrane pliki w dowolne miejsce. Dlatego w razie potrzeby skopiowania tylko kilku plików i folderów z kopii zapasowej woluminu nie ma konieczności przeprowadzania całej procedury odzyskiwania.

Przeglądanie zawartości obrazów

Przeglądanie zawartości zamontowanych woluminów umożliwia wyświetlanie i modyfikowanie zawartości woluminu (w przypadku zamontowania w trybie do odczytu i zapisu).

Aby przeglądać zawartość zamontowanego woluminu, wybierz go w tabeli i kliknij **Przeglądaj**. Pojawi się okno domyślnego menedżera plików, w którym można sprawdzić zawartość zamontowanego woluminu.

Odmontowywanie obrazów

Utrzymywanie zamontowanych woluminów wymaga dużej ilości zasobów systemowych. Zaleca się odmontowanie woluminów po wykonaniu niezbędnych operacji. Jeśli woluminy nie zostaną odmontowane ręcznie, pozostaną zamontowane do momentu ponownego uruchomienia systemu operacyjnego.

Aby odmontować obraz, wybierz go w tabeli i kliknij **Odmontuj**.

Aby odmontować wszystkie zamontowane woluminy, kliknij **Odmontuj wszystkie**.

6.7 Eksportowanie archiwów i kopii zapasowych

Operacja eksportu tworzy kopię archiwum lub samowystarczalną częściową kopię archiwum w lokalizacji określonej przez użytkownika. Oryginalne archiwum pozostaje nietknięte.

Operację eksportu można zastosować do następujących obiektów:

- **Jedno archiwum** — zostanie utworzona dokładna kopia archiwum.
- **Jedna kopia zapasowa** — zostanie utworzone archiwum składające się z jednej pełnej kopii zapasowej. Eksport przyrostowej lub różnicowej kopii zapasowej odbywa się przez konsolidację poprzednich kopii zapasowych z najbliższą pełną kopią zapasową.
- **Zestaw wybranych kopii zapasowych** należących do tego samego archiwum — w archiwum wynikowym będą się znajdować tylko określone kopie zapasowe. Konsolidacja jest wykonywana zgodnie z wymaganiami użytkownika, więc archiwum wynikowe może zawierać pełne, przyrostowe lub różnicowe kopie zapasowe.

- **Cały skarbiec**, który można wyeksportować za pomocą interfejsu wiersza polecenia. Aby uzyskać więcej informacji, zobacz Opis wiersza polecenia programu Acronis Backup & Recovery 10.

Scenariusze użycia

Eksport umożliwia wyodrębnienie określonej kopii zapasowej z łańcucha przyrostowych kopii zapasowych w celu szybkiego jej odzyskania, zapisania na nośniku wymiennym bądź odłączanym albo w innym celu.

Przykład. W przypadku tworzenia kopii zapasowej danych do lokalizacji zdalnej przez niestabilne połączenie sieciowe lub połączenie o niskiej przepustowości (np. podczas tworzenia kopii zapasowej przez sieć WAN przy użyciu sieci VPN), zaleca się zapisać początkową pełną kopię zapasową na nośnik odłączany. Następnie można przesłać nośnik do lokalizacji zdalnej. Tam kopia zapasowa zostanie wyeksportowana z nośnika na dysk docelowy. Kolejne przyrostowe kopie zapasowe, które zazwyczaj są znacznie mniejsze, będą mogły być przenoszone przez sieć.

W wyniku eksportu skarbca zarządzanego na nośnik odłączany otrzymuje się przenośny skarbiec niezarządzany, którego można użyć w ramach następujących scenariuszy:

- przechowywanie kopii skarbca lub najważniejszych archiwów w innej lokalizacji,
- fizyczny przewóz skarbca do odległego oddziału firmy,
- odzyskanie danych bez dostępu do węzła magazynowania w przypadku problemów komunikacji sieciowej lub awarii węzła magazynowania,
- odzyskanie samego węzła magazynowania.

Eksport ze skarbca znajdującego się na dysku twardym na urządzenie taśmowe może być uważany za proste etapowe tworzenie archiwum na żądanie.

Nazwa archiwum wynikowego

Domyślnie wyeksportowane archiwum dziedziczy nazwę oryginalnego archiwum. Ponieważ przechowywanie wielu archiwów o takich samych nazwach w tej samej lokalizacji nie jest wskazane, następujące czynności stosowane do domyślnej nazwy archiwum są niedostępne:

- eksportowanie części archiwum do tej samej lokalizacji
- eksportowanie archiwum lub jego części do lokalizacji, w której istnieje archiwum o tej samej nazwie
- eksportowanie archiwum lub jego części dwukrotnie do tej samej lokalizacji

W każdym z powyższych przypadków należy podać nazwę archiwum unikatową w folderze lub skarbcu docelowym. Jeśli trzeba ponownie wykonać zadanie eksportu przy użyciu tej samej nazwy archiwum, należy najpierw usunąć archiwum powstałe w wyniku poprzedniej operacji eksportu.

Opcje archiwum wynikowego

Domyślnie wyeksportowane archiwum dziedziczy opcje oryginalnego archiwum, w tym szyfrowanie i hasło. W przypadku eksportowania archiwum chronionego hasłem pojawi się monit o podanie hasła. Jeżeli oryginalne archiwum jest zaszyfrowane, zostanie zastosowane hasło w celu zaszyfrowania archiwum wynikowego.

Lokalizacje źródłowe i docelowe

Kiedy konsola jest podłączona do **komputera zarządzanego**, można wyeksportować archiwum lub jego część do i z dowolnej lokalizacji dostępnej dla agenta znajdującego się na komputerze. Dotyczy to skarbców osobistych, lokalnie podłączonych urządzeń taśmowych i nośników wymiennych, a w zaawansowanych wersjach produktu — zarządzanych i niezarządzanych skarbców centralnych.

Kiedy konsola jest podłączona do **serwera zarządzania**, dostępne są dwie metody eksportu:

- Eksport ze **skarbca zarządzanego**. Zadanie eksportu jest wykonywane przez węzeł magazynowania, który zarządza skarbcem. Miejscem docelowym może być udział sieciowy lub folder lokalny węzła magazynowania.
- Eksport z **niezarządzanego skarbca centralnego**. Zadanie eksportu jest wykonywane przez agenta zainstalowanego na komputerze zarządzanym określonym przez użytkownika. Miejscem docelowym może być dowolna lokalizacja, do której agent ma dostęp, w tym skarbiec zarządzany.

Wskazówka. *Podczas konfigurowania zadania eksportu danych do zarządzanego skarbca deduplikacji wybierz komputer, na którym zainstalowany jest dodatek deduplikacji do agenta. W przeciwnym razie zadanie eksportu zakończy się niepowodzeniem.*

Operacja na zadaniach eksportu

Zadanie eksportu jest uruchamiane natychmiast po zakończeniu jego konfiguracji. Zadanie eksportu można zatrzymać lub usunąć tak samo jak każde inne zadanie.

Ukończone zadanie eksportu można uruchomić ponownie w dowolnej chwili. Przedtem należy usunąć archiwum utworzone w wyniku uruchomienia poprzedniego zadania, jeśli to archiwum nadal istnieje w skarbcu docelowym. W przeciwnym razie zadanie zakończy się niepowodzeniem. Nie można edytować zadania eksportu w celu określenia innej nazwy archiwum docelowego (to jest ograniczenie).

Wskazówka. *Można zastosować scenariusz etapowy ręcznie, regularnie wykonując zadanie usuwania archiwum, a po nim zadanie eksportu.*

Różne metody tworzenia zadania eksportu

Zadanie eksportu można najprościej utworzyć za pomocą strony **Eksport**. Ta strona umożliwia wyeksportowanie dowolnej kopii zapasowej lub dowolnego archiwum, które są dostępne dla użytkownika.

Dostęp do strony **Eksport** można uzyskać z widoku **Skarbce**. Kliknij prawym przyciskiem myszy obiekt do wyeksportowania (archiwum lub kopia zapasowa) i wybierz **Eksport** z menu kontekstowego. Zostanie otwarta strona **Eksport** ze wstępnie wybranym obiektem jako źródłem. Wystarczy tylko wybrać miejsce docelowe i (opcjonalnie) podać nazwę zadania.

Aby wyeksportować archiwum lub kopię zapasową, wykonaj poniższe czynności.

Ogólne

Nazwa zadania

[Opcjonalnie] Wprowadź unikatową nazwę zadania. Dobrze dobrana nazwa umożliwi szybką identyfikację zadania pośród innych zadań.

Poświadczenia zadania (s. 282)

[Opcjonalnie] Zadanie eksportu będzie uruchamiane w imieniu użytkownika, który je utworzył. W razie potrzeby można zmienić poświadczenia zadania. Aby uzyskać dostęp do tej opcji, zaznacz pole wyboru **Widok zaawansowany**.

Elementy do wyeksportowania

Eksportuj

Wybierz obiekt do wyeksportowania:

Archiwum (s. 252) — w tym przypadku należy określić tylko archiwum.

Kopia zapasowa (s. 284) — najpierw należy określić archiwum, a następnie wybrać żądane kopie zapasowe znajdujące się w tym archiwum.

Poświadczenia dostępu (s. 284)

[Opcjonalnie] Jeśli konto zadania nie ma wystarczających uprawnień dostępu do źródła, podaj poświadczenia dostępu. Aby uzyskać dostęp do tej opcji, zaznacz pole wyboru **Widok zaawansowany**.

Lokalizacja eksportu

Archiwum (s. 284)

Wprowadź ścieżkę do lokalizacji tworzonego archiwum.

Należy podać charakterystyczną nazwę i komentarz do nowego archiwum.

Poświadczenia dostępu (s. 286)

[Opcjonalnie] Jeśli poświadczenia zadania nie są wystarczające, podaj poświadczenia dostępu do lokalizacji docelowej. Aby uzyskać dostęp do tej opcji, zaznacz pole wyboru **Widok zaawansowany**.

Po wykonaniu wszystkich wymaganych czynności kliknij **OK**, aby rozpocząć zadanie eksportu.

6.7.1 Poświadczenia zadania

Określ poświadczenia konta, na którym zadanie będzie uruchamiane.

Aby określić poświadczenia

1. Wybierz jedną z następujących opcji:
   - **Użyj poświadczeń bieżącego użytkownika**

     Zadanie będzie uruchamiane przy użyciu poświadczeń, z którymi zalogował się użytkownik rozpoczynający zadania. Jeśli zadanie ma zostać uruchomione według harmonogramu, w momencie zakończenia tworzenia zadania użytkownik zostanie poproszony o aktualne hasło użytkownika.
   - **Użyj następujących poświadczeń**

     Zadanie będzie zawsze uruchamiane przy użyciu poświadczeń określonych przez użytkownika, niezależnie od tego, czy zadanie będzie uruchamiane ręcznie, czy wykonywane według harmonogramu.

     Określ:
     - **Nazwa użytkownika**. Wprowadzając nazwę konta użytkownika usługi Active Directory, należy określić również nazwę domeny (DOMENA\Nazwa_użytkownika lub Nazwa_użytkownika@domena).
     - **Hasło**. Hasło dla konta.
2. Kliknij **OK**.

Więcej informacji na temat używania poświadczeń w programie Acronis Backup & Recovery 10 można znaleźć w sekcji Właściciele i poświadczenia (s. 35).

Aby dowiedzieć się więcej na temat operacji dostępnych w zależności od uprawnień użytkownika, zobacz sekcję Uprawnienia użytkownika na komputerze zarządzanym (s. 34).

6.7.2 Wybór archiwum

Aby wybrać archiwum

1. Wprowadź pełną ścieżkę do lokalizacji w polu Ścieżka lub wybierz odpowiedni folder w drzewie folderów.
   - Jeśli archiwum znajduje się w magazynie Acronis Online Backup Storage, kliknij **Zaloguj** i określ poświadczenia logowania do magazynu online. Następnie rozwiń grupę **Magazyn kopii zapasowych online** i wybierz konto.

   W przypadku kopii zapasowych zapisanych w magazynie Acronis Online Backup Storage nie są obsługiwane operacje eksportowania i montowania.

   - Jeśli archiwum znajduje się w skarbcu centralnym, rozwiń grupę **Centralne** i kliknij skarbiec.
   - Jeśli archiwum znajduje się w skarbcu osobistym, rozwiń grupę **Osobiste** i kliknij skarbiec.
   - Jeśli archiwum znajduje się w folderze lokalnym na komputerze, rozwiń grupę **Foldery lokalne** i kliknij odpowiedni folder.

   Jeśli archiwum znajduje się na nośniku wymiennym, na przykład na płycie DVD, najpierw włóż ostatnią płytę DVD, a następnie zgodnie z wyświetlanymi monitami wkładaj kolejno pozostałe płyty, zaczynając od pierwszej.

   - Jeśli archiwum znajduje się w udziale sieciowym, rozwiń grupę **Foldery sieciowe**, wybierz żądany komputer sieciowy, a następnie kliknij folder udostępniony. Jeśli udział sieciowy wymaga poświadczeń dostępu, program wyświetli odpowiedni monit.

   ***Uwaga dla użytkowników systemu Linux:** Aby określić udział sieciowy CIFS (Common Internet File System) zamontowany w punkcie montowania, takim jak /mnt/share, należy wybrać ten punkt montowania, a nie sam udział sieciowy.*

   - Jeśli archiwum znajduje się na serwerze **FTP** lub **SFTP**, w polu **Ścieżka** wpisz nazwę lub adres serwera w następujący sposób:

     ftp://serwer_ftp:numer_portu lub sftp://serwer_sftp:numer_portu

     Jeśli nie określisz numeru portu, dla serwera FTP zostanie użyty port 21, a dla SFTP — 22.

     Po wprowadzeniu poświadczeń dostępu zostaną udostępnione foldery na serwerze. Kliknij odpowiedni folder.

     Dostęp do serwera można uzyskać jako użytkownik anonimowy, o ile serwer zezwala na taki dostęp. W tym celu nie trzeba wprowadzać poświadczeń, lecz należy kliknąć opcję **Użyj dostępu anonimowego**.

   Jak wynika z oryginalnej specyfikacji protokołu FTP, poświadczenia wymagane do uzyskania dostępu do serwerów FTP są przesyłane w sieci jako otwarty tekst. Oznacza to, że nazwę użytkownika i hasło można przejąć przy użyciu programu do przechwytywania pakietów.

   - Jeśli archiwum znajduje się na podłączonym lokalnie urządzeniu taśmowym, rozwiń grupę **Napędy taśmowe** i kliknij odpowiednie urządzenie.

   W przypadku serwera zarządzania w drzewie folderów wybierz skarbiec zarządzany.
2. Wybierz archiwum w tabeli po prawej stronie drzewa. Tabela przedstawia nazwy archiwów znajdujących się w każdym wybranym przez użytkownika skarbcu lub folderze. Jeśli archiwum jest chronione hasłem, podaj hasło.

   Gdy przeglądasz zawartość lokalizacji, inni użytkownicy lub sam program mogą dodać, usunąć lub zmodyfikować archiwa. Przycisk **Odśwież** pozwala odświeżyć listę archiwów.

3. Kliknij **OK**.

6.7.3 Wybór kopii zapasowej

Aby określić kopie zapasowe do wyeksportowania

1. U góry okna zaznacz odpowiednie pola wyboru.

   Aby się upewnić, że została wybrana właściwa kopia zapasowa, kliknij kopię i spójrz na dolną tabelę, w której są wyświetlane woluminy znajdujące się w wybranej kopii zapasowej.

   Aby uzyskać informacje na temat woluminu, kliknij go prawym przyciskiem myszy, a następnie wybierz **Informacja**.
2. Kliknij **OK**.

6.7.4 Poświadczenia dostępu do źródła

Określ poświadczenia wymagane w celu uzyskania dostępu do lokalizacji, w której znajduje się archiwum źródłowe (lub kopia zapasowa).

Aby określić poświadczenia

1. Wybierz jedną z następujących opcji:
   - **Użyj poświadczeń zadania**

     Program użyje poświadczeń konta zadania określonych w sekcji Ogólne w celu dostępu do lokalizacji.
   - **Użyj następujących poświadczeń**

     Program uzyska dostęp do lokalizacji przy użyciu określonych poświadczeń. Tej opcji należy użyć, gdy konto zadania nie ma uprawnień dostępu do lokalizacji. Konieczne może być podanie specjalnych poświadczeń dla udziału sieciowego lub skarbca węzła magazynowania.

     Określ:
     - **Nazwa użytkownika**. Wprowadzając nazwę konta użytkownika usługi Active Directory, należy określić również nazwę domeny (DOMENA\Nazwa_użytkownika lub Nazwa_użytkownika@domena).
     - **Hasło**. Hasło dla konta.
2. Kliknij **OK**.

Jak wynika z oryginalnej specyfikacji protokołu FTP, poświadczenia wymagane do uzyskania dostępu do serwerów FTP są przesyłane w sieci jako otwarty tekst. Oznacza to, że nazwę użytkownika i hasło można przejąć przy użyciu programu do przechwytywania pakietów.

6.7.5 Wybór lokalizacji

Określ miejsce docelowe przechowywania wyeksportowanego obiektu. Eksportowanie kopii zapasowych do tego samego archiwum jest niedozwolone.

1. Wybór miejsca docelowego eksportu

Wprowadź pełną ścieżkę do miejsca docelowego w polu **Ścieżka** lub wybierz miejsce docelowe w drzewie folderów.

- Aby wyeksportować dane do niezarządzanego skarbca centralnego, rozwiń grupę **Skarbce centralne** i kliknij skarbiec.
- Aby wyeksportować dane do skarbca osobistego, rozwiń grupę **Skarbce osobiste** i kliknij skarbiec.

- Aby wyeksportować dane do folderu lokalnego na komputerze, rozwiń grupę **Foldery lokalne** i kliknij żądany folder.
- Aby wyeksportować dane do udziału sieciowego, rozwiń grupę **Foldery sieciowe**, wybierz żądany komputer sieciowy, a następnie kliknij folder udostępniony. Jeśli udział sieciowy wymaga poświadczeń dostępu, program wyświetli odpowiedni monit.

  Uwaga dla użytkowników systemu Linux: *Aby określić udział sieciowy CIFS (Common Internet File System) zamontowany w punkcie montowania, takim jak /mnt/share, należy wybrać ten punkt montowania, a nie sam udział sieciowy.*

- Aby wyeksportować dane na serwer **FTP** lub **SFTP**, wpisz nazwę i adres serwera w polu **Ścieżka** w następujący sposób:

  ftp://serwer_ftp:numer_portu lub **sftp://serwer_sftp:numer_portu**

  Jeśli nie określisz numeru portu, dla serwera FTP zostanie użyty port 21, a dla SFTP — 22.

  Po wprowadzeniu poświadczeń dostępu zostaną udostępnione foldery na serwerze. Kliknij odpowiedni folder.

  Dostęp do serwera można uzyskać jako użytkownik anonimowy, o ile serwer zezwala na taki dostęp. W tym celu nie trzeba wprowadzać poświadczeń, lecz należy kliknąć opcję **Użyj dostępu anonimowego**.

  Zgodnie z oryginalną specyfikacją protokołu FTP poświadczenia wymagane do uzyskania dostępu do serwerów FTP są przesyłane w sieci jako zwykły tekst. Oznacza to, że nazwę użytkownika i hasło można przechwycić przy użyciu programu do przechwytywania pakietów.

- Aby wyeksportować dane na lokalnie podłączone urządzenie taśmowe, rozwiń grupę **Napędy taśmowe**, a następnie kliknij żądane urządzenie.

W przypadku serwera zarządzania drzewo folderów zawiera:

- grupę Foldery lokalne dla potrzeb eksportu danych na lokalne dyski twarde węzła magazynowania;
- grupę Foldery sieciowe dla potrzeb eksportu danych do udziału sieciowego. Jeśli udział sieciowy wymaga poświadczeń dostępu, program wyświetli odpowiedni monit.

  Uwaga dla użytkowników systemu Linux: Aby określić udział sieciowy CIFS (Common Internet File System) zamontowany w punkcie montowania, takim jak /mnt/share, należy wybrać ten punkt montowania, a nie sam udział sieciowy.

2. Korzystanie z tabeli archiwów

Aby łatwiej było wybrać właściwe miejsce docelowe, w tabeli po prawej stronie są wyświetlane nazwy archiwów znajdujących się w poszczególnych lokalizacjach wybranych w drzewie.

Gdy przeglądasz zawartość lokalizacji, inni użytkownicy lub sam program mogą dodać, usunąć lub zmodyfikować archiwa. Przycisk **Odśwież** pozwala odświeżyć listę archiwów.

3. Nadawanie nazwy nowemu archiwum

Domyślnie wyeksportowane archiwum dziedziczy nazwę oryginalnego archiwum. Ponieważ przechowywanie wielu archiwów o takich samych nazwach w tej samej lokalizacji nie jest wskazane, następujące czynności stosowane do domyślnej nazwy archiwum są niedostępne:

- eksportowanie części archiwum do tej samej lokalizacji
- eksportowanie archiwum lub jego części do lokalizacji, w której istnieje archiwum o tej samej nazwie
- eksportowanie archiwum lub jego części dwukrotnie do tej samej lokalizacji

W każdym z powyższych przypadków należy podać nazwę archiwum unikatową w folderze lub skarbcu docelowym. Jeśli trzeba ponownie wykonać zadanie eksportu przy użyciu tej samej nazwy archiwum, należy najpierw usunąć archiwum powstałe w wyniku poprzedniej operacji eksportu.

6.7.6 Poświadczenia dostępu do miejsca docelowego

Określ poświadczenia wymagane w celu uzyskania dostępu do lokalizacji archiwum wynikowego. Właścicielem archiwum będzie użytkownik mający określoną nazwę.

Aby określić poświadczenia

1. Wybierz jedną z następujących opcji:
   - **Użyj poświadczeń zadania**

     Program użyje poświadczeń konta zadania określonych w sekcji Ogólne w celu dostępu do lokalizacji.
   - **Użyj następujących poświadczeń**

     Program uzyska dostęp do lokalizacji przy użyciu określonych poświadczeń. Tej opcji należy użyć, gdy konto zadania nie ma uprawnień dostępu do lokalizacji. Konieczne może być podanie specjalnych poświadczeń dla udziału sieciowego lub skarbca węzła magazynowania.

     Określ:
     - **Nazwa użytkownika**. Wprowadzając nazwę konta użytkownika usługi Active Directory, należy określić również nazwę domeny (DOMENA\Nazwa_użytkownika lub Nazwa_użytkownika@domena).
     - **Hasło**. Hasło dla konta.
2. Kliknij **OK**.

Jak wynika z oryginalnej specyfikacji protokołu FTP, poświadczenia wymagane do uzyskania dostępu do serwerów FTP są przesyłane w sieci jako otwarty tekst. Oznacza to, że nazwę użytkownika i hasło można przejąć przy użyciu programu do przechwytywania pakietów.

6.8 Strefa Acronis Secure Zone

Strefa Acronis Secure Zone to bezpieczna partycja, która umożliwia przechowywanie archiwów kopii zapasowych na dysku zarządzanego komputera. Dzięki temu dysk można odzyskać na tym samym dysku, na którym znajduje się jego kopia zapasowa.

Dostęp do tej strefy mogą uzyskać pewne aplikacje systemu Windows, na przykład narzędzia do zarządzania dyskami firmy Acronis.

Aby dowiedzieć się więcej na temat zalet i ograniczeń wynikających z korzystania ze strefy Acronis Secure Zone, zobacz temat Acronis Secure Zone (s. 60) w sekcji „Zastrzeżone technologie firmy Acronis”.

6.8.1 Tworzenie strefy Acronis Secure Zone

Strefę Acronis Secure Zone można utworzyć w działającym systemie operacyjnym lub przy użyciu nośnika startowego.

Aby utworzyć strefę Acronis Secure Zone, wykonaj poniższe czynności.

Miejsce

Dysk (s. 287)

Wybierz dysk twardy (jeśli jest ich kilka), na którym chcesz utworzyć strefę. Program tworzy strefę Acronis Secure Zone, wykorzystując nieprzydzielone miejsce na dysku lub wolne miejsce na woluminie.

Rozmiar (s. 287)

Określ dokładny rozmiar strefy. Przeniesienie lub zmiana rozmiaru zablokowanych woluminów, na przykład woluminu zawierającego aktywny system operacyjny, wymaga ponownego uruchomienia komputera.

Ustawienia

Hasło (s. 288)

[Opcjonalnie] Zabezpiecz strefę Acronis Secure Zone przed nieupoważnionym dostępem przy użyciu hasła. Podczas każdej operacji związanej ze strefą pojawi się monit o podanie hasła.

Po skonfigurowaniu wymaganych ustawień kliknij OK. W oknie Potwierdzenie wyniku (s. 288) sprawdź oczekiwany układ i kliknij OK, aby rozpocząć tworzenie strefy.

Dysk strefy Acronis Secure Zone

Strefa Acronis Secure Zone może znajdować się na dowolnym stałym dysku twardym. Strefa Acronis Secure Zone jest zawsze tworzona na końcu dysku twardego. Na komputerze może istnieć tylko jedna strefa Acronis Secure Zone. Jest ona tworzona przy użyciu ewentualnego nieprzydzielonego miejsca lub wolnego miejsca na woluminie.

Strefy Acronis Secure Zone nie można założyć na dysku dynamicznym ani na dysku, na którym stosowany jest styl partycjonowania GPT.

Aby przydzielić miejsce dla strefy Acronis Secure Zone

1. Wybierz dysk twardy (jeśli jest ich kilka), na którym chcesz utworzyć strefę. Domyślnie zostanie wybrane nieprzydzielone miejsce. Program wyświetli łączną ilość miejsca dostępnego dla strefy Acronis Secure Zone.
2. Chcąc przydzielić strefie więcej miejsca, wybierz woluminy, z których ma pochodzić wolne miejsce. W zależności od dokonanego wyboru program ponownie wyświetli łączną ilość miejsca dostępnego dla strefy Acronis Secure Zone. W oknie **Rozmiar strefy Acronis Secure Zone** (s. 287) możesz ustawić dokładny rozmiar strefy.
3. Kliknij **OK**.

Rozmiar strefy Acronis Secure Zone

Wprowadź rozmiar strefy Acronis Secure Zone lub przeciągnij suwak w celu wybrania dowolnego rozmiaru między wartościami minimalną i maksymalną. Rozmiar minimalny wynosi około 50 MB, w zależności od geometrii dysku twardego. Rozmiar maksymalny jest równy sumie ilości nieprzydzielonego miejsca na dysku oraz łącznej ilości wolnego miejsca na wszystkich woluminach, które zostały wybrane w poprzednim kroku.

Przydzielając miejsce z woluminu startowego lub systemowego, należy pamiętać o następujących kwestiach:

- Przeniesienie lub zmiana nazwy woluminu, z którego aktualnie uruchamiany jest system, wymaga ponownego uruchomienia systemu.

- Przydzielenie całego wolnego miejsca z woluminu systemowego może spowodować, że system operacyjny będzie działać niestabilnie lub nawet przestanie się uruchamiać. W przypadku wybrania woluminu startowego lub systemowego nie należy ustawiać maksymalnego rozmiaru strefy.

Hasło strefy Acronis Secure Zone

Ustawienie hasła chroni strefę Acronis Secure Zone przed nieupoważnionym dostępem. Podczas każdej operacji związanej ze strefą i znajdującymi się w niej archiwami, takiej jak tworzenie kopii zapasowej i odzyskiwanie danych, sprawdzanie poprawności archiwów, zmiana rozmiaru lub usuwanie strefy, program wyświetli monit o podanie hasła

Aby ustawić hasło

1. Wybierz **Użyj hasła**.
2. W polu **Wprowadź hasło** wpisz nowe hasło.
3. W polu **Potwierdź hasło** wpisz ponownie hasło.
4. Kliknij **OK**.

Aby wyłączyć hasło

1. Wybierz **Nie używaj**.
2. Kliknij **OK**.

Potwierdzenie wyniku

W oknie **Potwierdzenie wyniku** jest wyświetlany spodziewany układ partycji na podstawie wybranych ustawień. Jeśli układ jest zadowalający, kliknij **OK,** co spowoduje rozpoczęcie tworzenia strefy Acronis Secure Zone.

Wpływ wprowadzonych ustawień

W tej sekcji objaśniono, w jaki sposób utworzenie strefy Acronis Secure Zone wpływa na dysk zawierający wiele woluminów.

- Strefa Acronis Secure Zone jest zawsze tworzona na końcu dysku twardego. Podczas obliczania ostatecznego układu woluminów program najpierw wykorzystuje nieprzydzielone miejsce na końcu dysku.
- Jeśli na końcu dysku nie ma wystarczającej ilości nieprzydzielonego miejsca, ale istnieje ono między woluminami, woluminy są przenoszone w celu zwiększenia ilości nieprzydzielonego miejsca na końcu dysku.
- Jeśli mimo zgromadzenia całego nieprzydzielonego miejsca jego ilość jest wciąż niewystarczająca, program zajmuje wolne miejsce na woluminach wybranych przez użytkownika, zmniejszając odpowiednio rozmiary tych woluminów. Zmiana rozmiaru zablokowanych woluminów wymaga ponownego uruchomienia systemu.
- Na woluminie powinno jednak pozostać wolne miejsce, wymagane do prawidłowego działania systemu operacyjnego i aplikacji (na przykład do tworzenia plików tymczasowych). Program nie zmniejszy rozmiaru woluminu, na którym ilość wolnego miejsca jest lub stałaby się mniejsza niż 25% rozmiaru woluminu. Dopiero wówczas, gdy wszystkie woluminy na dysku będą zawierać 25% lub mniej wolnego miejsca, proporcjonalne zmniejszanie rozmiaru woluminów będzie kontynuowane.

Jak widać powyżej, nie warto ustawiać maksymalnego możliwego rozmiaru strefy. W efekcie na żadnym woluminie nie pozostanie wolne miejsce, skutkiem czego system operacyjny lub aplikacje mogą działać niestabilne lub w ogóle się nie uruchamiać.

6.8.2 Zarządzanie strefą Acronis Secure Zone

Strefa Acronis Secure Zone jest obsługiwana jako skarbiec osobisty (s. 428). Po utworzeniu na komputerze zarządzanym strefa jest zawsze obecna na liście **Skarbce osobiste**. Strefa Acronis Secure Zone może być używana w scentralizowanych planach tworzenia kopii zapasowych, a także w planach lokalnych.

Dotychczasowym użytkownikom strefy Acronis Secure Zone zwracamy uwagę na poważne zmiany w jej działaniu. Strefa nie wykonuje już automatycznego czyszczenia, czyli usuwania starych archiwów. Do tworzenia kopii zapasowych w strefie należy użyć schematów tworzenia kopii zapasowych z automatycznym czyszczeniem. Można również ręcznie usuwać nieaktualne kopie zapasowe przy użyciu funkcji zarządzania archiwami.

Nowy sposób działania strefy Acronis Secure Zone umożliwia:

- wyświetlanie listy archiwów znajdujących się w strefie i kopii zapasowych zawartych w każdym archiwum,
- sprawdzanie zawartości kopii zapasowej,
- montowanie kopii zapasowej woluminu w celu skopiowania plików z kopii zapasowej na dysk fizyczny,
- bezpieczne usuwanie archiwów oraz kopii zapasowych z archiwów.

Aby dowiedzieć się więcej na temat operacji na skarbcach, zobacz sekcję Skarbce (s. 144).

Zwiększanie strefy Acronis Secure Zone

Aby zwiększyć strefę Acronis Secure Zone

1. Na stronie **Zarządzaj strefą Acronis Secure Zone** kliknij **Zwiększ**.
2. Wybierz woluminy, których wolne miejsce chcesz wykorzystać do zwiększenia strefy Acronis Secure Zone.
3. Określ nowy rozmiar strefy:
   - Przeciągając suwak i wybierając dowolny rozmiar między wartościami bieżącą a maksymalną. Maksymalny rozmiar jest równy ilości nieprzydzielonego miejsca na dysku i łącznej ilości wolnego miejsca na wszystkich wybranych partycjach.
   - Wpisując dokładną wartość w polu Rozmiar strefy Acronis Secure Zone.

   Podczas zwiększania rozmiaru strefy program postępuje w poniższy sposób:
   - Najpierw wykorzystuje nieprzydzielone miejsce. W razie potrzeby program przenosi woluminy, ale nie zmienia ich rozmiaru. Przeniesienie zablokowanych woluminów wymaga ponownego uruchomienia komputera.
   - Jeśli ilość nieprzydzielonego miejsca jest niewystarczająca, program wykorzystuje wolne miejsce na wybranych woluminach, proporcjonalnie zmniejszając ich rozmiary. Zmiana rozmiaru zablokowanych partycji wymaga ponownego uruchomienia komputera.

   Zmniejszenie rozmiaru woluminu systemowego do minimalnej wielkości może uniemożliwić uruchomienie systemu operacyjnego komputera.
4. Kliknij **OK**.

Zmniejszanie strefy Acronis Secure Zone

Aby zmniejszyć strefę Acronis Secure Zone

1. Na stronie **Zarządzaj strefą Acronis Secure Zone** kliknij **Zmniejsz**.
2. Wybierz woluminy, do których chcesz dodać wolne miejsce po zmniejszeniu strefy.

3. Określ nowy rozmiar strefy:
   - Przeciągając suwak i wybierając dowolny rozmiar między wartościami bieżącą a minimalną. Minimalny rozmiar to około 50 MB, w zależności od geometrii dysku twardego.
   - Wpisując dokładną wartość w polu **Rozmiar strefy Acronis Secure Zone**.
4. Kliknij **OK**.

Usuwanie strefy Acronis Secure Zone

Aby usunąć strefę Acronis Secure Zone:

1. Na pasku **Działania dotyczące strefy Acronis Secure Zone** (w panelu **Czynności i narzędzia**) wybierz **Usuń**.
2. W oknie **Usuń strefę Acronis Secure Zone** wybierz woluminy, do których chcesz dodać miejsce zwolnione ze strefy, a następnie kliknij **OK**.

   W przypadku wybrania kilku woluminów miejsce zostanie rozłożone proporcjonalnie na każdej partycji. W przypadku niewybrania woluminu zwolnione miejsce stanie się nieprzydzielone.

Po kliknięciu **OK** program Acronis Backup & Recovery 10 rozpocznie usuwanie strefy.

6.9 Acronis Startup Recovery Manager

Program Acronis Startup Recovery Manager to zmodyfikowana wersja agenta startowego (s. 418), znajdująca się na dysku systemowym systemu Windows lub partycji /boot systemu Linux i uruchamiana po naciśnięciu klawisza F11 podczas uruchamiania komputera. Eliminuje on potrzebę użycia oddzielnego nośnika lub połączenia sieciowego w celu uruchomienia ratunkowego narzędzia startowego.

Aktywuj

Włącza monit startowy „Naciśnij klawisz F11, aby uruchomić Acronis Startup Recovery Manager” (jeśli nie ma programu ładującego GRUB) lub dodaje element „Acronis Startup Recovery Manager” do menu programu GRUB (jeśli program ten jest zainstalowany). Jeśli system nie uruchomi się, będzie można uruchomić ratunkowe narzędzie startowe, odpowiednio naciskając klawisz F11 lub wybierając narzędzie z menu.

Aktywacja programu Acronis Startup Recovery Manager. wymaga przynajmniej 70 MB wolnego miejsca na dysku systemowym (lub na partycji /boot w systemie Linux).

Jeśli nie jest używany program ładujący GRUB zainstalowany w głównym rekordzie rozruchowym (MBR), program Acronis Startup Recovery Manager podczas aktywacji zastępuje rekord MBR własnym kodem startowym. Dlatego konieczna może być ponowna aktywacja programów ładujących innych producentów, jeśli są one zainstalowane.

Jeśli w systemie Linux jest używany inny program ładujący niż GRUB (na przykład LILO), warto przed aktywacją programu ASRM zainstalować program ładujący w rekordzie rozruchowym partycji root (czyli rozruchowej) systemu Linux, a nie w głównym rekordzie rozruchowym. W przeciwnym razie należy ponownie skonfigurować program ładujący po aktywacji.

Nie aktywuj

Wyłącza monit startowy „Naciśnij klawisz F11, aby uruchomić Acronis Startup Recovery Manager” (lub odpowiedni element menu w programie GRUB). Jeśli program Acronis Startup Recovery Manager jest wyłączony, a system nie uruchomi się, w celu odzyskania systemu należy wykonać jedną z poniższych czynności:

- uruchomić komputer przy użyciu oddzielnego ratunkowego nośnika startowego,
- użyć funkcji uruchamiania przez sieć z serwera Acronis PXE Server lub za pomocą usługi instalacji zdalnej (RIS) firmy Microsoft.

Szczegółowe informacje znajdują się w sekcji Nośnik startowy (s. 291).

6.10 Nośnik startowy

Nośnik startowy

Nośnik startowy to nośnik fizyczny (CD, DVD, dysk USB lub inny nośnik obsługiwany przez system BIOS komputera jako urządzenie startowe), który uruchamia się na dowolnym komputerze kompatybilnym ze standardem PC i umożliwia uruchomienie agenta programu Acronis Backup & Recovery 10 w środowisku opartym na systemie Linux lub w środowisku preinstalacyjnym systemu Windows (WinPE) bez pomocy systemu operacyjnego. Nośnik startowy najczęściej jest stosowany w następujących przypadkach:

- odzyskiwanie systemu operacyjnego, którego nie można uruchomić;
- uzyskanie dostępu do danych ocalałych w uszkodzonym systemie i utworzenie ich kopii zapasowej;
- wdrożenie systemu operacyjnego po awarii;
- utworzenie podstawowych lub dynamicznych woluminów po awarii;
- utworzenie kopii zapasowej „sektor po sektorze” dysku z nieobsługiwanym systemem plików;
- utworzenie w trybie offline kopii zapasowej wszelkich danych, których kopii zapasowej nie można utworzyć w trybie online ze względu na ograniczony dostęp, trwałą blokadę założoną przez uruchomione aplikacje lub z jakichkolwiek innych powodów.

Komputer można uruchomić do powyższych środowisk za pomocą nośnika fizycznego albo przez sieć z serwera Acronis PXE Server, Windows Deployment Services (WDS) lub Remote Installation Services (RIS). Te serwery z przesłanymi na nie komponentami startowymi również mogą być traktowane jako pewnego rodzaju nośniki startowe. Używając tego samego kreatora, można utworzyć nośnik startowy bądź skonfigurować serwer PXE lub WDS/RIS.

Nośnik startowy oparty na systemie Linux

Nośnik oparty na systemie Linux zawiera agenta startowego Acronis Backup & Recovery 10 Bootable Agent opartego na jądrze systemu Linux. Agent może uruchamiać dowolny sprzęt kompatybilny ze standardem PC (w tym także systemy odzyskane po awarii i komputery z uszkodzonymi lub nieobsługiwanymi systemami plików) oraz wykonywać na nim operacje. Operacje mogą być konfigurowane i kontrolowane lokalnie lub zdalnie przy użyciu konsoli zarządzania.

Nośnik startowy oparty na środowisku PE

Nośnik startowy oparty na środowisku PE zawiera minimalną wersję systemu Windows nazywaną środowiskiem preinstalacyjnym systemu Windows (WinPE) oraz wtyczkę Acronis Plug-in for WinPE, to znaczy modyfikację agenta programu Acronis Backup & Recovery 10, która może być uruchamiana w środowisku preinstalacyjnym.

Środowisko WinPE jest najwygodniejszym rozwiązaniem startowym w dużych środowiskach wyposażonych w różnorodny sprzęt.

Zalety:

- Używanie programu Acronis Backup & Recovery 10 w środowisku preinstalacyjnym systemu Windows zapewnia większą funkcjonalność niż używanie nośnika startowego opartego na systemie Linux. Po uruchomieniu sprzętu kompatybilnego ze standardem PC do środowiska WinPE można używać nie tylko agenta programu Acronis Backup & Recovery 10, ale także poleceń i skryptów środowiska PE oraz innych wtyczek dodanych do środowiska PE.
- Nośnik startowy oparty na środowisku PE ułatwia pokonanie niektórych problemów z nośnikiem startowym dotyczących systemu Linux, takich jak obsługa niektórych kontrolerów RAID lub tylko niektórych poziomów macierzy RAID. Nośnik oparty na środowisku PE 2.x, tzn. na jądrze systemu Windows Vista lub Windows Server 2008, umożliwia dynamiczne ładowanie potrzebnych sterowników urządzeń.

6.10.1 Jak utworzyć nośnik startowy

Aby było możliwe tworzenie nośników fizycznych, komputer musi być wyposażony w nagrywarkę CD/DVD lub umożliwiać podłączenie dysku flash. Aby było możliwe konfigurowanie serwera PXE lub WDS/RIS, komputer musi być podłączony do sieci. Generator nośnika startowego umożliwia także utworzenie obrazu ISO dysku startowego, który później można będzie nagrać na czystej płycie.

Nośnik startowy oparty na systemie Linux

Uruchom Generator nośnika startowego (za pomocą konsoli zarządzania, wybierając **Narzędzia > Utwórz nośnik startowy**, lub jako oddzielny komponent).

Wybierz sposób obsługi woluminów i zasobów sieciowych (tzw. styl nośników):

- Nośnik obsługujący woluminy w stylu systemu Linux wyświetla woluminy jako np. hda1 i sdb2. Przed rozpoczęciem odzyskiwania próbuje zrekonstruować urządzenia MD i woluminy logiczne (LVM).
- Nośnik obsługujący woluminy w stylu systemu Windows wyświetla woluminy jako np. C: i D:. Zapewnia dostęp do woluminów dynamicznych (LDM).

Specjalny kreator pomoże w wykonaniu niezbędnych operacji. Aby uzyskać szczegółowe informacje, zobacz Nośnik startowy oparty na systemie Linux (s. 293).

Nośnik startowy oparty na środowisku PE

Wtyczkę Acronis Plug-in for WinPE można dodać do dystrybucji środowiska WinPE opartych na dowolnym z następujących jąder:

- Windows XP Professional z dodatkiem Service Pack 2 (PE 1.5)
- Windows Server 2003 z dodatkiem Service Pack 1 (PE 1.6)
- Windows Vista (PE 2.0)
- Windows Vista SP1 i Windows Server 2008 (PE 2.1)
- Windows 7 (PE 3.0)

Jeśli masz już nośnik z dystrybucją PE1.x, rozpakuj obraz ISO nośnika do folderu lokalnego i uruchom Generator nośnika startowego z konsoli zarządzania, wybierając **Narzędzia > Utwórz nośnik startowy**, lub jako osobny komponent. Specjalny kreator pomoże w wykonaniu niezbędnych operacji. Aby uzyskać szczegółowe informacje, zobacz Dodawanie wtyczki Acronis Plug-in do środowiska WinPE 1.x (s. 298).

Aby umożliwić tworzenie i modyfikowanie obrazów środowiska PE 2.x lub 3.0, należy zainstalować Generator nośnika startowego na komputerze, na którym jest zainstalowany zestaw zautomatyzowanej instalacji systemu Windows (Windows AIK). Dalsze operacje opisano w sekcji Dodawanie wtyczki Acronis Plug-in do środowiska WinPE 2.x lub 3.0 (s. 298).

Jeśli na komputerze nie jest zainstalowany zestaw Windows AIK, przygotuj się w następujący sposób:

1. Pobierz i zainstaluj zestaw zautomatyzowanej instalacji systemu Windows.

   Zestaw zautomatyzowanej instalacji systemu Windows Vista (PE 2.0):

   http://www.microsoft.com/Downloads/details.aspx?familyid=C7D4BC6D-15F3-4284-9123-679830D629F2&displaylang=pl

   Zestaw zautomatyzowanej instalacji systemów Windows Vista SP1 i Windows Server 2008 (PE 2.1):

   http://www.microsoft.com/downloads/details.aspx?FamilyID=94bb6e34-d890-4932-81a5-5b50c657de08&DisplayLang=pl

   Zestaw zautomatyzowanej instalacji systemu Windows 7 (PE 3.0):

   http://www.microsoft.com/downloads/details.aspx?familyid=696DD665-9F76-4177-A811-39C26D3B3B34&displaylang=pl

   Wymagania systemowe dotyczące instalacji można znaleźć, korzystając z powyższych łączy.
2. [Opcjonalnie] Nagraj zestaw zautomatyzowanej instalacji systemu Windows na płycie DVD lub skopiuj go na dysk flash.
3. Zainstaluj środowisko Microsoft .NET Framework 2.0 zawarte w tym zestawie (NETFXx86 lub NETFXx64, w zależności od posiadanego sprzętu).
4. Zainstaluj analizator Microsoft Core XML (MSXML) 5.0 lub 6.0 zawarty w tym zestawie.
5. Zainstaluj zestaw zautomatyzowanej instalacji systemu Windows zawarty w tym zestawie.
6. Zainstaluj Generator nośnika startowego na tym samym komputerze.

Zalecamy zapoznanie się z dokumentacją pomocy dostarczoną z zestawem zautomatyzowanej instalacji systemu Windows. Aby uzyskać dostęp do dokumentacji, z menu Start wybierz **Microsoft Windows AIK -> Dokumentacja**.

Korzystanie ze środowiska Bart PE

Używając generatora Bart PE Builder, można utworzyć obraz środowiska Bart PE z wtyczką Acronis Plug-in. Aby uzyskać szczegółowe informacje, zobacz Generowanie środowiska Bart PE z wtyczką Acronis Plug-in z dystrybucji systemu Windows (s. 300).

Nośnik startowy oparty na systemie Linux

W przypadku korzystania z generatora nośnika należy określić następujące elementy:

1. [Opcjonalnie] Parametry jądra systemu Linux. Kolejne parametry należy oddzielać spacjami.

   Aby móc wybrać tryb wyświetlania agenta startowego przy każdym uruchomieniu nośnika, należy wpisać **vga=ask**

   Lista parametrów znajduje się w sekcji Parametry jądra (s. 294).
2. Komponenty startowe Acronis, które zostaną umieszczone na nośniku.
   - Jeśli na komputerze, na którym jest tworzony nośnik, zainstalowano dodatek Acronis Backup & Recovery 10 Universal Restore, można go włączyć.
3. [Opcjonalnie] Wartość limitu czasu menu startowego oraz komponent, który będzie automatycznie uruchamiany po przekroczeniu tego limitu.

- Jeśli ta opcja nie zostanie skonfigurowana, program ładujący Acronis będzie czekał, aż użytkownik określi, czy ma być uruchamiany system operacyjny (jeśli istnieje), czy komponent Acronis.
- Jeśli ustawisz na przykład **10 s** dla agenta startowego, agent zostanie uruchomiony po upływie 10 s od wyświetlenia menu. Umożliwia to wykonanie nienadzorowanych operacji lokalnych podczas uruchamiania z serwera PXE lub WDS/RIS.

4. [Opcjonalnie] Ustawienia zdalnego logowania:
   - Nazwa użytkownika i hasło, które należy wprowadzić po stronie konsoli podczas nawiązywania połączenia z agentem. Jeśli te pola pozostaną puste, połączenie będzie włączane po wpisaniu dowolnych symboli w oknie monitu.
5. [Opcjonalnie] Ustawienia sieciowe (s. 296):
   - Ustawienia TCP/IP, które zostaną przypisane do kart sieciowych komputera.
6. [Opcjonalnie] Port sieciowy (s. 297):
   - Port TCP, na którym agent startowy nasłuchuje połączeń przychodzących.
7. Typ nośnika do utworzenia. Można:
   - utworzyć płytę CD lub DVD albo inny nośnik startowy, na przykład wymienny dysk flash USB, jeśli system BIOS umożliwia uruchamianie komputera z tego rodzaju nośników;
   - wygenerować obraz ISO dysku startowego, który później można będzie nagrać na czystej płycie;
   - przesłać wybrane komponenty na serwer Acronis PXE Server;
   - przesłać wybrane komponenty na serwer WDS/RIS.
8. [Opcjonalnie] Sterowniki systemu Windows, które będą używane przez dodatek Acronis Universal Restore. (s. 297) To okno jest wyświetlane tylko w przypadku, gdy zainstalowano dodatek Acronis Universal Restore i wybrano nośnik inny niż serwer PXE lub WDS/RIS.
9. Ścieżka do pliku ISO nośnika bądź nazwa lub adres IP i poświadczenia serwera PXE lub WDS/RIS.

Parametry jądra

To okno pozwala określić parametry jądra systemu Linux. Zostaną one automatycznie zastosowane po uruchomieniu nośnika startowego.

Parametry te są przeważnie używane w razie problemów z pracą z nośnika startowego. W standardowych sytuacjach pole to może pozostać puste.

Każdy z wpisywanych parametrów można także podać, naciskając przy starcie systemu klawisz F11.

Parametry

Jeśli chcesz określić wiele parametrów, rozdziel je spacjami.

acpi=off

Wyłącza interfejs zaawansowanego zarządzania energią ACPI. Warto użyć tego parametru, jeśli występują problemy z określoną konfiguracją sprzętową.

noapic

Wyłącza kontroler APIC. Warto użyć tego parametru, jeśli występują problemy z określoną konfiguracją sprzętową.

vga=ask

Wyświetla monit o wybór trybu obrazu używanego przez graficzny interfejs użytkownika nośnika startowego. W przypadku braku parametru **vga** tryb obrazu jest wybierany automatycznie.

vga=*numer_trybu*

Określa trybu obrazu używanego przez graficzny interfejs użytkownika nośnika startowego. Numer trybu jest określony wartością *numer_trybu* podaną w formacie szesnastkowym, na przykład **vga=0x318**

Rozdzielczość ekranu i liczba kolorów w wybranym trybie może zależeć od komputera. Aby wybrać odpowiednią wartość **numer_trybu**, zaleca się najpierw użycie parametru *vga=ask*.

quiet

Wyłącza wyświetlanie komunikatów startowych podczas ładowania jądra systemu Linux, a po jego załadowaniu uruchamia konsolę zarządzania.

Parametr ten jest pośrednio określony podczas tworzenia nośnika startowego, jednak w menu startowym można go usunąć.

Bez tego parametru zostaną wyświetlone wszystkie komunikaty startowe, a następnie pojawi się wiersz poleceń. Aby uruchomić z niego konsolę zarządzania, wpisz polecenie **/bin/product**

nousb

Wyłącza ładowanie podsystemu obsługi interfejsu USB.

nousb2

Wyłącza obsługę interfejsu USB 2.0. Urządzenia USB 1.1 będą nadal obsługiwane. Przy użyciu tego parametru można użyć w trybie USB 1.1 tych dysków USB, które nie działają w trybie USB 2.0.

nodma

Wyłącza funkcję bezpośredniego dostępu do pamięci (DMA) dla wszystkich dysków twardych IDE. Zapobiega zawieszaniu się jądra przy niektórych urządzeniach

nofw

Wyłącz obsługę interfejsu FireWire (IEEE1394).

nopcmcia

Wyłącza rozpoznawanie urządzeń PCMCIA.

nomouse

Wyłącza obsługę myszy.

*nazwa_modułu***=off**

Wyłącza moduł określony w parametrze *nazwa_modułu*. Aby na przykład wyłączyć obsługę modułu SATA, określ **sata_sis=off**

pci=bios

Wymusza obsługę systemu BIOS interfejsu PCI zamiast bezpośredniej. Użyj tego parametru, jeśli komputer jest wyposażony w niestandardowy mostek obsługi urządzeń PCI.

pci=nobios

Wyłącza obsługę systemu BIOS interfejsu PCI. Możliwy będzie wyłącznie bezpośredni dostęp do urządzeń. Użyj tego parametru, jeśli występują problemy z uruchomieniem nośnika startowego, które mogą być spowodowane przez system BIOS.

pci=biosirq

Uzyskuje tabelę przekierowywania przerwań za pomocą wywołań systemu BIOS interfejsu PCI. Użyj tego parametru, jeśli jądro nie może przydzielić żądań przerwań (IRQ) lub odnaleźć dodatkowych magistrali PCI na płycie głównej.

Wywołania te mogą nie działać prawidłowo na niektórych komputerach. Jednak może być to jedyny sposób uzyskania tabeli przekierowywania przerwań.

Ustawienia sieciowe

Podczas tworzenia nośnika startowego Acronis można wstępnie skonfigurować połączenia sieciowe, których będzie używał agent startowy. Można wstępnie skonfigurować następujące parametry:

- adres IP,
- maska podsieci,
- brama,
- serwer DNS,
- serwer WINS.

Gdy agent startowy uruchamia się na komputerze, konfiguracja jest stosowana do karty interfejsu sieciowego (NIC) komputera. Jeśli ustawienia nie zostały wstępnie skonfigurowane, agent używa automatycznej konfiguracji DHCP. Ustawienia sieciowe można także skonfigurować ręcznie, gdy agent startowy jest uruchomiony na komputerze.

Wstępne konfigurowanie wielu połączeń sieciowych

Można wstępnie skonfigurować ustawienia TCP/IP dla maksymalnie dziesięciu kart interfejsu sieciowego. Aby zagwarantować przypisanie odpowiednich ustawień do każdej karty, należy utworzyć nośnik na serwerze, do którego zostanie on dostosowany. Po wybraniu istniejącej karty interfejsu sieciowego w oknie kreatora zostaną zaznaczone jej ustawienia, które zostaną zapisane na nośniku. Na nośniku zostanie także zapisany adres MAC każdej istniejącej karty interfejsu sieciowego.

Ustawienia, z wyjątkiem adresu MAC, można zmienić. Jeśli istnieje taka potrzeba, można także skonfigurować ustawienia nieistniejącej karty interfejsu sieciowego.

Gdy agent startowy uruchamia się na serwerze, pobiera listę dostępnych kart interfejsu sieciowego. Lista jest posortowana według gniazd zajmowanych przez karty: karta znajdująca się najbliżej procesora jest wyświetlana na górze listy.

Agent startowy przypisuje do każdej znanej karty interfejsu sieciowego odpowiednie ustawienia, identyfikując karty na podstawie ich adresów MAC. Po skonfigurowaniu kart interfejsu sieciowego o znanych adresach MAC do pozostałych kart są przypisywane ustawienia, które zostały wprowadzone dla nieistniejących kart, począwszy od najwyższej nieprzypisanej karty interfejsu sieciowego.

Nośnik startowy można dostosować do dowolnego komputera, a nie tylko do komputera, na którym został utworzony. Aby to zrobić, należy skonfigurować karty interfejsu sieciowego zgodnie z kolejnością ich gniazd na tym komputerze: NIC1 zajmuje gniazdo najbliżej procesora, w następnym gnieździe znajduje się NIC2 itd. Gdy agent startowy będzie uruchamiał się na tym komputerze, nie

znajdzie żadnych kart o znanych adresach MAC i skonfiguruje karty w takiej samej kolejności jak użytkownik.

Przykład

Agent startowy może używać jednej z kart sieciowych do komunikacji z konsolą zarządzania przez sieć produkcyjną. Na potrzeby tego połączenia można utworzyć konfigurację automatyczną. Duże ilości danych odzyskiwania można przesyłać za pośrednictwem drugiej karty, uwzględnionej w dedykowanej sieci tworzenia kopii zapasowych za pomocą ustawień statycznego adresu TCP/IP.

Port sieciowy

Podczas tworzenia nośnika startowego można wstępnie skonfigurować port sieciowy, na którym będzie nasłuchiwał agent startowy, aby uzyskać informacje o połączeniu przychodzącym. Dostępne opcje to:

- port domyślny,
- aktualnie używany port,
- nowy port (należy wprowadzić numer portu).

Jeśli port nie został wstępnie skonfigurowany, agent używa domyślnego numeru portu (9876). Ten port jest także używany domyślnie przez konsolę zarządzania Acronis Backup & Recovery 10 Management Console.

Sterowniki dodatku Universal Restore

Podczas tworzenia nośnika startowego można dodać do nośnika sterowniki systemu Windows. Sterowniki będą używane przez dodatek Universal Restore podczas odzyskiwania systemu Windows na komputerze z innym procesorem, inną płytą główną lub innym urządzeniem pamięci masowej niż w systemie, którego kopia zapasowa została utworzona.

Dodatek Universal Restore można skonfigurować:

- aby wyszukiwać na nośniku sterowniki, które najlepiej pasują do sprzętu docelowego;
- aby pobierać z nośnika jawnie określone sterowniki pamięci masowej. Jest to konieczne, gdy sprzęt docelowy jest wyposażony w określony kontroler pamięci dyskowej masowej (na przykład kartę SCSI, RAID lub Fiber Channel).

Aby uzyskać więcej informacji, zobacz Universal Restore (s. 262).

Sterowniki zostaną umieszczone w widocznym folderze Drivers na nośniku startowym. Sterowniki nie są ładowane do pamięci RAM komputera docelowego, dlatego w czasie pracy dodatku Universal Restore nośnik musi być włożony lub podłączony.

Dodawanie sterowników do nośnika startowego jest dostępne pod warunkiem, że:

1. na komputerze, na którym jest tworzony nośnik startowy, zainstalowano dodatek Acronis Backup & Recovery 10 Universal Restore; ORAZ
2. użytkownik tworzy nośnik wymienny, jego obraz ISO lub nośnik odłączany, taki jak dysk flash. Nie można przesłać sterowników na serwer PXE ani WDS/RIS.

Sterowniki można dodawać do listy wyłącznie w grupach, dodając pliki INF lub foldery zawierające takie pliki. Nie można wybierać pojedynczych sterowników z plików INF, ale generator nośnika pokazuje zawartość pliku dla celów informacyjnych.

Aby dodać sterowniki:

1. Kliknij **Dodaj** i znajdź plik INF lub folder zawierający pliki INF.
2. Wybierz plik INF lub folder.
3. Kliknij **OK**.

Sterowniki można usuwać z listy wyłącznie w grupach, usuwając pliki INF.

Aby usunąć sterowniki:

1. Wybierz plik INF.
2. Kliknij **Usuń**.

Dodawanie wtyczki Acronis Plug-in do środowiska WinPE 1.x

Wtyczkę Acronis Plug-in for WinPE można dodać do środowiska:

- Windows PE 2004 (1.5) (system Windows XP Professional z dodatkiem Service Pack 2),
- Windows PE 2005 (1.6) (system Windows Server 2003 z dodatkiem Service Pack 1).

Aby dodać wtyczkę Acronis Plug-in do środowiska WinPE 1.x:

1. Rozpakuj wszystkie pliki z obrazu ISO środowiska WinPE 1.x do oddzielnego folderu na dysku twardym.
2. Uruchom Generator nośnika startowego (za pomocą konsoli zarządzania, wybierając **Narzędzia > Utwórz nośnik startowy**, lub jako oddzielny komponent).
3. Wybierz **Typ nośnika startowego: Windows PE**.
   - Wybierz polecenie **Użyj plików WinPE znajdujących się w określonym folderze**.
4. Określ ścieżkę do folderu zawierającego pliki WinPE.
5. Określ ustawienia sieciowe (s. 296) kart sieciowych komputera lub wybierz automatyczną konfigurację DHCP.
6. Określ pełną ścieżkę do wynikowego pliku ISO, łącznie z nazwą pliku.
7. Na ekranie podsumowania sprawdź ustawienia i kliknij **Kontynuuj**.
8. Nagraj obraz ISO na płycie CD lub DVD za pomocą narzędzia innej firmy albo skopiuj obraz na dysk flash.

Po uruchomieniu komputera w środowisku WinPE automatycznie uruchomi się program Acronis Backup & Recovery 10.

Dodawanie wtyczki Acronis Plug-in do środowiska WinPE 2.x lub 3.0

Generator nośnika startowego oferuje trzy metody integracji programu Acronis Backup & Recovery 10 ze środowiskiem WinPE 2.x lub 3.0:

- dodanie wtyczki Acronis Plug-in do istniejącego obrazu ISO środowiska PE — możliwość przydatna, gdy wtyczkę trzeba dodać do wcześniej skonfigurowanego i już używanego obrazu ISO środowiska PE;
- utworzenie od podstaw obrazu ISO środowiska PE z wtyczką;
- dodanie wtyczki Acronis Plug-in do pliku WIM do dowolnych przyszłych celów (ręczne generowanie obrazu ISO, dodawanie innych narzędzi do obrazu itd.).

Aby umożliwić wykonanie dowolnej z tych operacji, należy zainstalować Generator nośnika startowego na komputerze, na którym jest zainstalowany zestaw zautomatyzowanej instalacji systemu Windows. Jeśli taki komputer nie istnieje, należy przygotować go w sposób opisany w sekcji Jak utworzyć nośnik startowy (s. 292).

Generator nośnika startowego obsługuje tylko środowisko WinPE 2.x lub 3.0 x86. Te dystrybucje środowiska WinPE mogą także działać na sprzęcie o architekturze x64.

Obraz PE oparty na środowisku Win PE 2.0 wymaga do działania co najmniej 256 MB pamięci RAM. Zalecany rozmiar pamięci w przypadku środowiska PE 2.0 wynosi 512 MB. Obraz PE oparty na środowisku Win PE 3.0 wymaga do działania co najmniej 512 MB pamięci RAM.

Dodawanie wtyczki Acronis Plug-in do obrazu ISO środowiska WinPE 2.x lub 3.0

Aby dodać wtyczkę Acronis Plug-in do obrazu ISO środowiska WinPE 2.x lub 3.0:

1. W przypadku dodawania wtyczki do istniejącego obrazu ISO środowiska Win PE należy rozpakować wszystkie pliki tego obrazu do oddzielnego folderu na dysku twardym.
2. Uruchom Generator nośnika startowego (za pomocą konsoli zarządzania, wybierając **Narzędzia > Utwórz nośnik startowy**, lub jako oddzielny komponent).
3. Wybierz **Typ nośnika startowego: Windows PE**.

   W przypadku tworzenia nowego obrazu ISO środowiska PE:

   - Wybierz **Utwórz automatycznie środowisko Windows PE 2.x lub 3.0**.
   - Program uruchomi odpowiedni skrypt i przejdzie do następnego okna.

   W trakcie dodawania wtyczki do istniejącego obrazu ISO środowiska PE:

   - Wybierz polecenie **Użyj plików WinPE znajdujących się w określonym folderze**.
   - Określ ścieżkę do folderu zawierającego pliki WinPE.
4. Określ ustawienia sieciowe (s. 296) kart sieciowych komputera lub wybierz automatyczną konfigurację DHCP.
5. [Opcjonalnie] Określ sterowniki systemu Windows, które mają być dodane do środowiska Windows PE. Po uruchomieniu komputera w środowisku Windows PE sterowniki ułatwiają dostęp do urządzenia, na którym znajduje się archiwum kopii zapasowej. Kliknij **Dodaj** i określ ścieżkę do niezbędnego pliku *.inf dla odpowiedniego kontrolera SCSI, RAID, SATA, karty sieciowej, napędu taśmowego lub innego urządzenia. Procedurę tę należy powtórzyć w przypadku każdego sterownika, który ma być dołączony do wynikowego nośnika startowego środowiska WinPE.
6. Wybierz, czy utworzyć obraz ISO lub WIN, albo prześlij nośnik na serwer Acronis PXE.
7. Określ pełną ścieżkę do wynikowego pliku obrazu (włącznie z nazwą pliku) lub określ serwer PXE i podaj nazwę użytkownika i hasło, aby uzyskać do niego dostęp.
8. Na ekranie podsumowania sprawdź ustawienia i kliknij **Kontynuuj**.
9. Nagraj obraz ISO na płycie CD lub DVD za pomocą narzędzia innej firmy albo skopiuj obraz na dysk flash.

Po uruchomieniu komputera w środowisku WinPE automatycznie uruchomi się program Acronis Backup & Recovery 10.

Aby utworzyć obraz środowiska PE (plik ISO) z wynikowego pliku WIM:

- Zastąp domyślny plik boot.wim w folderze Windows PE nowo utworzonym plikiem WIM. W powyższym przykładzie wpisz:

  ```
  copy c:\AcronisMedia.wim c:\winpe_x86\ISO\sources\boot.wim
  ```

- Używanie narzędzia **Oscdimg**. W powyższym przykładzie wpisz:

  ```
  oscdimg -n –bc:\winpe_x86\etfsboot.com c:\winpe_x86\ISO
  c:\winpe_x86\winpe_x86.iso
  ```

Aby uzyskać więcej informacji na temat dostosowywania środowiska Windows PE, zobacz Windows Preinstallation Environment User's Guide (Podręcznik użytkownika środowiska preinstalacyjnego systemu Windows) (Winpe.chm).

Generowanie środowiska Bart PE z wtyczką Acronis Plug-in z dystrybucji systemu Windows

1. Uzyskaj generator środowiska Bart PE.
2. Zainstaluj Generator nośnika startowego z pliku instalacyjnego programu Acronis Backup & Recovery 10.
3. Zmień bieżący folder na folder, w którym jest zainstalowana wtyczka Acronis Plug-in for WinPE — domyślnie: C:\Program Files\Acronis\Bootable Components\WinPE.

   Jeśli wtyczka jest zainstalowana w folderze innym niż domyślny, zmień odpowiednio ścieżkę (aby poznać lokalizację wtyczki, sprawdź klucz rejestru HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\Bootable Components\Settings\WinPE).
4. Rozpakuj plik WinPE.zip do bieżącego folderu.
5. Uruchom następujące polecenie:

   ```
   export_license.bat
   ```
6. Skopiuj zawartość bieżącego folderu — domyślnie: C:\Program Files\Acronis\Bootable Components\WinPE — do folderu %Folder BartPE%\plugins\Acronis.
7. Jeśli na dysku twardym nie masz kopii plików instalacyjnych systemu Windows, włóż płytę CD z dystrybucją tego systemu.
8. Uruchom generator środowiska Bart PE.
9. Określ ścieżkę do plików instalacyjnych systemu Windows lub płyty CD z dystrybucją systemu Windows.
10. Kliknij **Plugins** (Wtyczki) i sprawdź, czy jest włączona wtyczka programu Acronis Backup & Recovery 10. Jeśli jest wyłączona, włącz ją.
11. Określ folder wyjściowy i pełną ścieżkę do wynikowego pliku ISO, łącznie z nazwą pliku lub nośnikiem do utworzenia.
12. Wygeneruj środowisko Bart PE.
13. Nagraj obraz ISO na płycie CD lub DVD (jeśli ta czynność nie została jeszcze wykonana) albo skopiuj go na dysk flash.

Po uruchomieniu komputera w środowisku Bart PE i skonfigurowaniu połączenia sieciowego wybierz **Go -> System -> Storage -> Acronis Backup & Recovery 10** (Przejdź -> System -> Magazyn -> Acronis <PRODUCT NAME>) w celu rozpoczęcia pracy.

6.10.2 Łączenie z komputerem uruchamianym z nośnika

Po uruchomieniu komputera z nośnika startowego terminal komputera wyświetla okno uruchamiania z adresami IP uzyskanymi z serwera DHCP lub ustawionymi zgodnie ze wstępnie skonfigurowanymi wartościami.

Połączenie zdalne

Aby podłączyć komputer zdalnie, należy wybrać **Połącz -> Zarządzaj komputerem zdalnym** w menu konsoli i określić jeden z adresów IP komputera. Należy także podać nazwę użytkownika i hasło, jeśli zostały one skonfigurowane podczas tworzenia nośnika startowego.

Połączenie lokalne

Na nośniku startowym zawsze jest obecna konsola Acronis Backup & Recovery 10 Management Console. Każdy użytkownik, który ma fizyczny dostęp do terminalu komputera, może uruchomić konsolę i nawiązać połączenie. Wystarczy kliknąć **Uruchom konsolę zarządzania** w oknie uruchamiania agenta startowego.

6.10.3 Praca na nośniku startowym

Operacje wykonywane na komputerze uruchamianym za pomocą nośnika startowego są bardzo podobne do operacji tworzenia kopii zapasowych i odzyskiwania w systemie operacyjnym. Różnice są następujące:

1. Litery dysków widoczne podczas pracy z nośnikiem startowym w stylu systemu Windows mogą różnić się od sposobu identyfikacji dysków przez system Windows. Na przykład dysk D: w narzędziu ratunkowym może odpowiadać dyskowi E: w systemie Windows.

   Ostrożnie! Dla bezpieczeństwa zaleca się przypisywanie unikatowych nazw woluminów.

2. Na nośniku startowym w stylu systemu Linux dyski i woluminy lokalne są pokazywane jako odmontowane (sda1, sda2...).
3. Nośnik startowy w stylu systemu Linux nie może zapisać kopii zapasowej na woluminie sformatowanym w systemie NTFS. W razie potrzeby należy przełączyć się na styl Windows.
4. Aby przełączać nośnik startowy między stylami Linux i Windows, wybierz **Narzędzia** > **Zmień reprezentację woluminu**.
5. W graficznym interfejsie użytkownika nośnika nie ma drzewa **Nawigacja**. Do przechodzenia między widokami służy element menu **Nawigacja**.
6. Nie można planować zadań. Tak naprawdę w ogóle nie można tworzyć zadań. Jeśli trzeba powtórzyć operację, należy skonfigurować ją od początku.
7. Czas życia dziennika jest ograniczony do bieżącej sesji. Cały dziennik lub odfiltrowane wpisy dziennika można zapisać w pliku.
8. Skarbce centralne nie są wyświetlane w drzewie folderów okna **Archiwum**.

   Aby uzyskać dostęp do skarbca zarządzanego, w polu **Ścieżka** wpisz następujący ciąg:

   bsp://adres_węzła/nazwa_skarbca/

   Aby uzyskać dostęp do niezarządzanego skarbca centralnego, wpisz pełną ścieżkę do folderu skarbca.

   Po wprowadzeniu poświadczeń dostępu zostanie wyświetlona lista archiwów znajdujących się w skarbcu.

Konfigurowanie trybu wyświetlania

W przypadku komputera uruchamianego z nośnika tryb wyświetlania obrazu wideo jest wykrywany automatycznie na podstawie konfiguracji sprzętowej (parametrów monitora i karty graficznej). Jeśli z jakiegoś powodu tryb wideo jest wykrywany niepoprawnie, wykonaj następujące czynności:

1. W menu startowym naciśnij F11.
2. Wstaw w wierszu polecenia następujące polecenie: **vga=ask**, a następnie kontynuuj uruchamianie.
3. Z listy obsługiwanych trybów wideo wybierz odpowiedni tryb, wpisując jego numer (na przykład **318**), a następnie naciśnij ENTER.

Jeśli nie chcesz wykonywać tej procedury przy każdym uruchamianiu danej konfiguracji sprzętowej z nośnika startowego, ponownie utwórz nośnik, wprowadzając odpowiedni numer trybu (w tym

przykładzie — **vga=0x318**) w oknie **Parametry jądra** (szczegółowe informacje znajdują się w sekcji Generator nośnika startowego (s. 293)).

Konfigurowanie urządzeń iSCSI i NDAS

W tej sekcji znajduje się opis konfigurowania urządzeń iSCSI i NDAS podczas pracy z nośnikiem startowym.

Urządzenia te są podłączane do komputera przez interfejs sieciowy i wyglądają jak urządzenia podłączane lokalnie. Urządzenia iSCSI są w sieci rozpoznawane po swoich adresach IP, a urządzenia NDAS — po identyfikatorach.

Urządzenia iSCSI są czasami nazywane obiektami docelowymi iSCSI. Komponent sprzętowy lub programowy, który zapewnia interakcję między komputerem i obiektem docelowym iSCSI, nazywany jest inicjatorem iSCSI. Nazwa inicjatora iSCSI jest z reguły definiowana przez administratora serwera, który służy jako host urządzenia.

Aby dodać urządzenie iSCSI

1. Z nośnika startowego (opartego na systemie Linux lub środowisku PE) uruchom konsolę zarządzania.
2. Kliknij **Skonfiguruj urządzenia iSCSI/NDAS** (w przypadku nośnika opartego na systemie Linux) lub **Uruchom konfigurację iSCSI** (w przypadku nośnika opartego na środowisku PE).
3. Określ adres IP i port hosta urządzenia iSCSI oraz nazwę inicjatora iSCSI.
4. Jeśli host wymaga uwierzytelniania, określ odpowiednią nazwę użytkownika i hasło.
5. Kliknij **OK**.
6. Wybierz urządzenie iSCSI z listy i kliknij **Połącz**.
7. Jeśli pojawi się monit, określ nazwę użytkownika i hasło umożliwiające dostęp do urządzenia iSCSI.

Aby dodać urządzenie NDAS

1. Z nośnika startowego opartego na systemie Linux uruchom konsolę zarządzania.
2. Kliknij **Skonfiguruj urządzenia iSCSI/NDAS**.
3. W sekcji **Urządzenia NDAS** kliknij **Dodaj urządzenie**.
4. Określ 20-znakowy identyfikator urządzenia.
5. Jeśli chcesz umożliwić zapis danych w urządzeniu, podaj pięcioznakowy klucz zapisu. Bez tego klucza urządzenie będzie dostępne w trybie tylko do odczytu.
6. Kliknij **OK**.

6.10.4 Lista poleceń i narzędzi dostępnych na nośniku startowym opartym na systemie Linux

Nośnik startowy oparty na systemie Linux zawiera poniższe polecenia i narzędzia wiersza polecenia, których można używać po uruchomieniu powłoki poleceń. Aby uruchomić powłokę poleceń, w konsoli zarządzania nośnika startowego naciśnij klawisze CTRL+ALT+F2.

Narzędzia wiersza polecenia w oprogramowaniu Acronis

- `acronis`
- `asamba`
- `lash`
- `restoreraids`

- `trueimagecmd`
- `trueimagemnt`

Polecenia i narzędzia systemu Linux

`busybox`	`ifconfig`	`rm`
`cat`	`init`	`rmmod`
`cdrecord`	`insmod`	`route`
`chmod`	`iscsiadm`	`scp`
`chown`	`kill`	`scsi_id`
`chroot`	`kpartx`	`sed`
`cp`	`ln`	`sg_map26`
`dd`	`ls`	`sh`
`df`	`lspci`	`sleep`
`dmesg`	`lvm`	`ssh`
`dmraid`	`mdadm`	`sshd`
`e2fsck`	`mkdir`	`strace`
`e2label`	`mke2fs`	`swapoff`
`echo`	`mknod`	`swapon`
`egrep`	`mkswap`	`sysinfo`
`fdisk`	`more`	`tar`
`fsck`	`mount`	`tune2fs`
`fxload`	`mtx`	`udev`
`gawk`	`mv`	`udevinfo`
`gpm`	`pccardctl`	`udevstart`
`grep`	`ping`	`umount`
`growisofs`	`pktsetup`	`uuidgen`
`grub`	`poweroff`	`vconfig`
`gunzip`	`ps`	`vi`
`halt`	`raidautorun`	`zcat`
`hexdump`	`readcd`	
`hotplug`	`reboot`	

6.10.5 Odzyskiwanie urządzeń MD i woluminów logicznych

Aby odzyskać urządzenia MD, zwane programowymi urządzeniami RAID systemu Linux, i/lub urządzenia utworzone w Menedżerze woluminów logicznych (LVM), zwane woluminami logicznymi, przed rozpoczęciem odzyskiwania należy utworzyć odpowiednią strukturę woluminów.

Strukturę woluminów można utworzyć na jeden z następujących sposobów:

- Automatycznie za pomocą nośnika startowego z systemem Linux, przy użyciu konsoli zarządzania lub skryptu — zobacz Automatyczne tworzenie struktury woluminów (s. 304).
- Ręcznie za pomocą narzędzi **mdadm** i **lvm** — zobacz Ręczne tworzenie struktury woluminów (s. 305).

Automatyczne tworzenie struktury woluminów

Przyjmijmy, że struktura woluminu jest zapisana (s. 52) w katalogu /etc/Acronis i wolumin wraz z tym katalogiem jest dołączony do archiwum.

Aby odtworzyć strukturę woluminów na nośniku startowym z systemem Linux należy użyć jednej z poniższych metod.

Uwaga: *Wskutek wykonania poniższych procedur istniejąca w komputerze struktura woluminów zostanie zastąpiona nową, przechowywaną w archiwum. Spowoduje to zniszczenie wszystkich danych znajdujących się obecnie na niektórych lub wszystkich dyskach twardych komputera.*

W przypadku zmiany konfiguracji dysków Urządzenie MD lub wolumin logiczny znajduje się na przynajmniej jednym dysku, przy czym każdy dysk może mieć inny rozmiar. Jeśli doszło do zastąpienia dowolnego z dysków w czasie między utworzeniem kopii zapasowej a odzyskiwaniem lub woluminy są odzyskiwane na inny komputer, sprawdź, czy w nowej konfiguracji dysków znajduje się wystarczająca liczba dysków o rozmiarach nie mniejszych niż rozmiary poprzednich dysków.

Aby utworzyć strukturę woluminów za pomocą konsoli zarządzania

1. Uruchom komputer z nośnika startowego opartego na systemie Linux.
2. Kliknij **Acronis Agent startowy**. Następnie kliknij **Uruchom konsolę zarządzania**.
3. W konsoli zarządzania kliknij **Odzyskaj**.

   W sekcji z zawartością archiwum program Acronis Backup & Recovery 10 wyświetli komunikat o wykryciu informacji o strukturze woluminu.
4. W obszarze komunikatu kliknij **Szczegóły**.
5. Zapoznaj się ze strukturą woluminu i, aby ją utworzyć, kliknij **Zastosuj RAID/LVM**.

Aby utworzyć strukturę woluminu za pomocą skryptu

1. Uruchom komputer z nośnika startowego opartego na systemie Linux.
2. Kliknij **Acronis Agent startowy**. Następnie kliknij **Uruchom konsolę zarządzania**.
3. Na pasku narzędzi kliknij **Czynności**, a następnie kliknij **Uruchom powłokę**. Możesz również nacisnąć klawisze CTRL+ALT+F2.
4. Uruchom skrypt **restoreraids.sh**, określając pełną nazwę pliku archiwum, na przykład:

   ```
   /bin/restoreraids.sh
   smb://server/backups/linux_machine_2010_01_02_12_00_00_123D.tib
   ```
5. Wróć do konsoli zarządzania, naciskając klawisze CTRL+ALT+F1 lub uruchamiając polecenie: **/bin/product**
6. Kliknij **Odzyskaj**, określ ścieżkę do archiwum i wszystkie inne wymagane parametry, a następnie kliknij **OK**.

Jeśli program Acronis Backup & Recovery 10 nie może utworzyć struktury woluminu (lub brak jej w archiwum), utwórz strukturę ręcznie.

Ręczne tworzenie struktury woluminów

Poniżej przedstawiono ogólną procedurę odzyskiwania urządzeń MD i woluminów logicznych przy użyciu nośnika startowego opartego na systemie Linux oraz przykład takiego odzyskiwania. W systemie Linux można zastosować podobną procedurę.

Aby odzyskać urządzenia MD i woluminy logiczne

1. Uruchom komputer z nośnika startowego opartego na systemie Linux.
2. Kliknij **Acronis Agent startowy**. Następnie kliknij **Uruchom konsolę zarządzania**.
3. Na pasku narzędzi kliknij **Czynności**, a następnie kliknij **Uruchom powłokę**. Możesz również nacisnąć klawisze CTRL+ALT+F2.
4. W razie potrzeby sprawdź strukturę woluminów przechowywanych w archiwum, używając narzędzia **trueimagecmd**. Ponadto możesz użyć narzędzia **trueimagemnt**, aby zamontować jeden lub więcej tych woluminów tak, jakby były zwykłymi woluminami (zobacz „Montowanie woluminów z kopii zapasowych” w dalszej części tego tematu).
5. Utwórz strukturę woluminów zgodnie ze strukturą zawartą w archiwum, używając narzędzia **mdadm** (w przypadku urządzeń MD), narzędzia **lvm** (w przypadku woluminów logicznych) lub obu tych narzędzi.

   Uwaga: *Narzędzia Menedżera woluminów logicznych takie jak **pvcreate** i **vgcreate**, zazwyczaj dostępne w systemie Linux, nie są dołączane do środowiska nośnika startowego, dlatego należy użyć narzędzia **lvm** z odpowiednim poleceniem: **lvm pvcreate**, **lvm vgcreate** itp.*
6. Jeśli wcześniej kopia zapasowa została zamontowana przy użyciu narzędzia **trueimagemnt**, użyj tego narzędzia ponownie, aby odmontować kopię zapasową (zobacz „Montowanie woluminów z kopii zapasowych” w dalszej części tego tematu).
7. Wróć do konsoli zarządzania, naciskając klawisze CTRL+ALT+F1 lub uruchamiając polecenie: **/bin/product**

   (W tym momencie nie uruchamiaj ponownie komputera. W przeciwnym razie konieczne będzie ponowne utworzenie struktury woluminów).
8. Kliknij **Odzyskaj**, określ ścieżkę do archiwum i wszystkie inne wymagane parametry, a następnie kliknij **OK**.

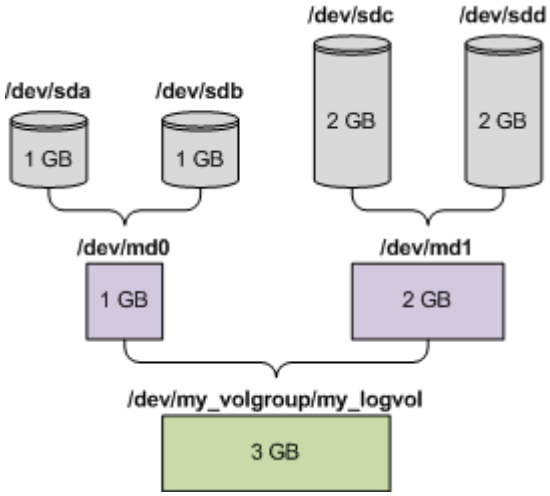
Uwaga: *Ta procedura nie ma zastosowania po nawiązaniu zdalnego połączenia z agentem startowym programu Acronis Backup & Recovery 10, ponieważ w takim przypadku powłoka poleceń jest niedostępna.*

Przykład

Załóżmy, że została wykonana kopia zapasowa dysku komputera o następującej konfiguracji dysków:

- Komputer zawiera dwa dyski twarde SCSI o pojemności 1 GB i dwa takie dyski o pojemności 2 GB, zamontowane odpowiednio w partycjach **/dev/sda**, **/dev/sdb**, **/dev/sdc** i **/dev/sdd**.
- Pierwszą i drugą parę dysków twardych skonfigurowano jako dwa urządzenia MD (oba w konfiguracji RAID-1) i zamontowano odpowiednio w partycjach **/dev/md0** i **/dev/md1**.
- Wolumin logiczny opiera się na tych dwóch urządzeniach MD i jest zamontowany w partycji **/dev/my_volgroup/my_logvol**.

Konfigurację tę przedstawia poniższa ilustracja.



Aby odzyskać dane z tego archiwum, wykonaj poniższe czynności.

Krok 1: Utworzenie struktury woluminów

1. Uruchom komputer z nośnika startowego opartego na systemie Linux.
2. W konsoli zarządzania naciśnij klawisze CTRL+ALT+F2.
3. Uruchom następujące polecenia, aby utworzyć urządzenia MD:

   ```
   mdadm --create /dev/md0 --level=1 --raid-devices=2 /dev/sd[ab]
   mdadm --create /dev/md1 --level=1 --raid-devices=2 /dev/sd[cd]
   ```

4. Uruchom następujące polecenia, aby utworzyć grupę woluminu logicznego:

   Przestroga: *Polecenie* ***pvcreate*** *niszczy wszystkie dane na urządzeniach* ***/dev/md0*** *i* ***/dev/md1****.*

   ```
   lvm pvcreate /dev/md0 /dev/md1
   lvm vgcreate my_volgroup /dev/md0 /dev/md1
   lvm vgdisplay
   ```

   Dane wyjściowe polecenia **lvm vgdisplay** będą zawierać wiersze podobne do przedstawionych poniżej:

   ```
   --- Volume group ---
   VG Name     my_volgroup
   ...
   VG Access   read/write
   VG Status   resizable
   ...
   VG Size     1.99 GB
   ...
   VG UUID     0qoQ4l-Vk7W-yDG3-uF1l-Q2AL-C0z0-vMeACu
   ```

5. Uruchom poniższe polecenie, aby utworzyć wolumin logiczny. W parametrze **-L** określ rozmiar podany jako **VG Size**:

   ```
   lvm lvcreate -L1.99G --name my_logvol my_volgroup
   ```

6. Aktywuj grupę woluminu, uruchamiając następujące polecenie:

   ```
   lvm vgchange -a y my_volgroup
   ```

7. Naciśnij klawisze CTRL+ALT+F1, aby wrócić do konsoli zarządzania.

Krok 2: Rozpoczęcie odzyskiwania

1. W konsoli zarządzania kliknij **Odzyskaj**.

2. W obszarze **Archiwum** kliknij **Zmień**, a następnie określ nazwę archiwum.
3. W obszarze **Kopia zapasowa** kliknij **Zmień**, a następnie wybierz kopię zapasową, z której chcesz odzyskać dane.
4. W obszarze **Typ danych** wybierz **Woluminy**.
5. W obszarze **Elementy do odzyskania** zaznacz pole wyboru obok pozycji **my_volgroup-my_logvol**.
6. W obszarze **Lokalizacja odzyskiwania** kliknij **Zmień**, a następnie wybierz wolumin utworzony w kroku 1. Listę dysków możesz rozwijać przyciskami strzałek.
7. Kliknij **OK**, aby rozpocząć odzyskiwanie.

Aby uzyskać pełną listę poleceń i narzędzi, których można używać w środowisku nośnika startowego, zobacz Lista poleceń i narzędzi dostępnych na nośniku startowym opartym na systemie Linux (s. 302). Aby uzyskać szczegółowe opisy narzędzi **trueimagecmd** i **trueimagemnt**, zobacz opis wiersza polecenia programu Acronis Backup & Recovery 10.

Montowanie woluminów z kopii zapasowych

Zamontowanie woluminu przechowywanego w kopii zapasowej dysku może być konieczne na przykład w celu wyświetlenia niektórych zawartych w nim plików przed rozpoczęciem odzyskiwania.

Aby zamontować wolumin kopii zapasowej

1. Za pomocą polecenia **--list** wyświetl listę woluminów przechowywanych w kopii zapasowej. Na przykład:

   ```
   trueimagecmd --list --filename:smb://server/backups/linux_machine.tib
   ```

   Dane wyjściowe będą zawierać wiersze podobne do przedstawionych poniżej:

   ```
   Num  Idx Partition Flags Start Size      Type
   ---- --- --------- ----- ----- --------- ------
   Disk 1:
            Table           0               Table
   Disk 2:
            Table           0               Table
   ...
   Woluminy dynamiczne i GPT:
   DYN1 4   my_volgroup-my_logvol 12533760  Ext2
   ```

   Indeks woluminu podany w kolumnie **Indeks** będzie potrzebny w następnym kroku.

2. Użyj polecenia **--mount**, określając indeks woluminu w parametrze **-i**. Na przykład:

   ```
   trueimagemnt --mount /mnt --filename smb://server/backups/linux_machine.tib -i
   4
   ```

   To polecenie spowoduje zamontowanie woluminu logicznego DYN1, którego indeks w kopii zapasowej ma wartość 4, w punkcie montowania /mnt.

Aby odmontować wolumin kopii zapasowej

- Użyj polecenia **--unmount**, określając punkt montowania woluminu jako parametr. Na przykład:

  ```
  trueimagemnt --unmount /mnt
  ```

6.10.6 Acronis PXE Server

Serwer Acronis PXE Server umożliwia uruchamianie komputerów na komponentach startowych Acronis za pośrednictwem sieci.

Uruchamianie przez sieć:

- eliminuje potrzebę lokalnej obecności technika w celu zainstalowania nośnika startowego w systemie, który ma zostać uruchomiony;
- w czasie operacji grupowych skraca czas potrzebny do uruchomienia wielu komputerów (w porównaniu z korzystaniem z fizycznego nośnika startowego).

Komponenty startowe są przesyłane na serwer Acronis PXE Server przy użyciu Generatora nośnika startowego Acronis. Aby przesłać komponenty startowe, uruchom Generator nośnika startowego (za pomocą konsoli zarządzania, wybierając **Narzędzia > Utwórz nośnik startowy**, lub jako oddzielny komponent) i wykonaj szczegółowe instrukcje opisane w sekcji „Generator nośnika startowego (s. 293)”.

Uruchamianie wielu komputerów z serwera Acronis PXE Server ma sens, jeśli w sieci znajduje się serwer DHCP (Dynamic Host Control Protocol). Dzięki niemu interfejsy sieciowe uruchamianych komputerów automatycznie uzyskują adresy IP.

Instalacja serwera Acronis PXE Server

Aby zainstalować serwer Acronis PXE Server:

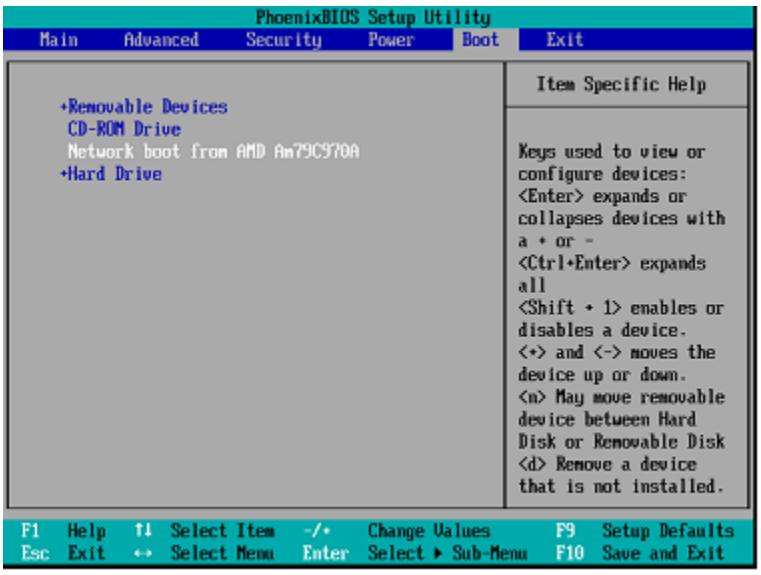
1. Uruchom plik instalacyjny programu Acronis Backup & Recovery 10.
2. Z listy **Komponenty do zarządzania scentralizowanego** wybierz serwer Acronis PXE Server.
3. Postępuj zgodnie z wyświetlanymi instrukcjami.

Serwer Acronis PXE Server uruchamia się jako usługa natychmiast po zainstalowaniu. W późniejszym czasie uruchamia się automatycznie przy każdym ponownym uruchomieniu systemu. Serwer Acronis PXE Server można zatrzymywać i uruchamiać w taki sam sposób jak inne usługi systemu Windows.

Konfigurowanie komputera na potrzeby uruchamiania z serwera PXE

W przypadku systemu odzyskanego po awarii wystarczy, że system BIOS komputera obsługuje uruchamianie przez sieć.

Na komputerze z systemem operacyjnym na dysku twardym należy skonfigurować system BIOS tak, aby karta interfejsu sieciowego była pierwszym urządzeniem startowym lub przynajmniej urządzeniem uruchamianym przed dyskiem twardym. Poniższy przykład przedstawia jedną z właściwych konfiguracji systemu BIOS. Jeśli do komputera nie zostanie włożony nośnik startowy, komputer uruchomi się z sieci.



W niektórych wersjach systemu BIOS po włączeniu karty interfejsu sieciowego należy zapisać zmiany, aby karta pojawiła się na liście urządzeń startowych.

Jeśli komputer jest wyposażony w wiele kart interfejsu sieciowego, należy się upewnić, że do karty obsługiwanej przez system BIOS podłączono kabel sieciowy.

PXE i DHCP na tym samym serwerze

Jeśli serwer Acronis PXE Server i serwer DHCP znajdują się na tym samym komputerze, należy dodać do serwera DHCP opcję 60: „Identyfikator klienta” z wartością ciągu „PXE Client”. Można to zrobić w następujący sposób:

```
C:\WINDOWS\system32>netsh
netsh>dhcp
netsh>dhcp>server \\<nazwa_serwera> lub <adres IP>
netsh dhcp>add optiondef 60 PXEClient STRING 0 comment=”Opcja dodana w celu obsługi serwera PXE”
netsh dhcp>set optionvalue 60 STRING PXEClient
```

Praca w podsieciach

Aby umożliwić pracę serwera Acronis PXE Server w innej podsieci (przez przełącznik), należy skonfigurować przełącznik tak, aby przekazywał ruch na serwerze PXE. Adresy IP serwera PXE są konfigurowane na bazie interfejsów przy użyciu funkcji pomocnika IP w taki sam sposób jak adresy serwera DHCP. Aby uzyskać więcej informacji, zobacz: http://support.microsoft.com/kb/257579/pl.

6.11 Zarządzanie dyskami

Acronis Disk Director Lite to narzędzie do przygotowywania konfiguracji dysków/woluminów komputera na potrzeby odzyskiwania obrazów woluminów zapisanych przez oprogramowanie Acronis Backup & Recovery 10.

Czasami po utworzeniu kopii zapasowej woluminu i umieszczeniu jego obrazu w bezpiecznym miejscu przechowywania konfiguracja dysków komputera może ulec zmianie z powodu wymiany dysku twardego lub utraty sprzętu. W takim przypadku za pomocą narzędzia Acronis Disk Director Lite można odtworzyć niezbędną konfigurację dysków, pozwalającą na odzyskanie obrazu woluminu w dokładnie takiej samej postaci, jaką miał on wcześniej. Można też wprowadzić dowolną zmianę struktury dysków lub woluminów, którą użytkownik uzna za niezbędną.

Wszystkie operacje na dyskach lub woluminach wiążą się z pewnym ryzykiem uszkodzenia danych. Operacje na woluminach systemowych, startowych lub woluminach danych należy wykonywać bardzo ostrożnie, aby uniknąć potencjalnych problemów z procesem uruchamiania lub magazynowaniem danych na dysku twardym.

Operacje związane z dyskami twardymi i woluminami zajmują trochę czasu, a każda przerwa w dopływie zasilania, niezamierzone wyłączenie komputera lub przypadkowe naciśnięcie przycisku Reset podczas wykonywania procedury może spowodować uszkodzenie woluminu i utratę danych.

Wszelkie operacje na woluminach dysków dynamicznych w systemach Windows XP i Windows 2000 można wykonywać tylko po uruchomieniu usługi Acronis Managed Machine Service na koncie z uprawnieniami administratora.

Aby uniknąć możliwej utraty danych, należy zastosować wszystkie niezbędne środki ostrożności (s. 310).

6.11.1 Podstawowe środki ostrożności

Aby uniknąć możliwego uszkodzenia struktury dysków i woluminów lub utraty danych, należy zastosować wszystkie niezbędne środki ostrożności oraz przestrzegać następujących prostych reguł:

1. Utwórz kopię zapasową dysku, na którym będzie się odbywało tworzenie woluminów lub zarządzanie nimi. Utworzenie kopii zapasowej najważniejszych danych na innym dysku twardym, w udziale sieciowym lub na nośniku wymiennym zagwarantuje bezpieczeństwo danych podczas pracy z woluminami dysku.
2. Sprawdź dysk, aby upewnić się, że jest w pełni sprawny i nie zawiera uszkodzonych sektorów ani błędów systemu plików.
3. Nie wykonuj żadnych operacji na dyskach/woluminach, gdy są uruchomione inne programy mające dostęp do dysków na niskim poziomie. Przed uruchomieniem narzędzia Acronis Disk Director Lite zamknij te programy.

Te proste środki ostrożności zapewniają ochronę przed przypadkową utratą danych.

6.11.2 Uruchamianie narzędzia Acronis Disk Director Lite

Narzędzie Acronis Disk Director Lite można uruchomić w systemie Windows lub z nośnika startowego.

Uruchamianie narzędzia Acronis Disk Director Lite w systemie Windows

Po uruchomieniu konsoli zarządzania Acronis Backup & Recovery 10 Management Console i podłączeniu jej do komputera zarządzanego, w drzewie **Nawigacja** konsoli będzie dostępny widok **Zarządzanie dyskami**, w którym można uruchomić narzędzie Acronis Disk Director Lite.

Uruchamianie narzędzia Acronis Disk Director Lite z nośnika startowego

Narzędzie Acronis Disk Director Lite można uruchomić w systemie odzyskanym po awarii, na komputerze, którego nie można uruchomić, albo na komputerze z systemem innym niż Windows. W tym celu należy uruchomić komputer z nośnika startowego (s. 424) utworzonego za pomocą generatora nośnika startowego Acronis, a następnie uruchomić konsolę zarządzania i kliknąć **Zarządzanie dyskami**.

6.11.3 Wybieranie systemu operacyjnego do zarządzania dyskami

Na komputerze, na którym znajdują się dwa lub więcej systemów operacyjnych, reprezentacja dysków i woluminów zależy od aktualnie uruchomionego systemu operacyjnego.

W różnych systemach operacyjnych Windows wolumin może mieć inną literę. Na przykład wolumin E: po uruchomieniu innego systemu operacyjnego Windows zainstalowanego na tym samym komputerze może być wyświetlany jako D: lub L:. (Jest także możliwe, że ten wolumin będzie miał tę samą literę E: w każdym systemie operacyjnym Windows zainstalowanym na komputerze).

Dysk dynamiczny utworzony w jednym systemie operacyjnym Windows może być uważany w innym systemie Windows za **dysk obcy** lub może w ogóle nie być obsługiwany przez ten system.

Aby wykonać na takim komputerze operację zarządzania dyskami, należy określić system operacyjny, dla którego będzie wyświetlany układ dysków i w którym będzie wykonywana operacja zarządzania dyskami.

Nazwa aktualnie wybranego systemu operacyjnego jest wyświetlana na pasku narzędzi konsoli za opcją „**Bieżący układ dysku**”. Aby wybrać inny system operacyjny w oknie **Wybór systemu operacyjnego**, należy kliknąć jego nazwę. Podczas pracy na nośniku startowym to okno pojawia się po kliknięciu **Zarządzanie dyskami**. Układ dysków będzie wyświetlany zgodnie z wybranym systemem operacyjnym.

6.11.4 Widok „Zarządzanie dyskami”

Do sterowania narzędziem Acronis Disk Director Lite służy widok **Zarządzanie dyskami** konsoli.

W górnej części widoku znajduje się tabela dysków i woluminów umożliwiająca sortowanie danych i dostosowywanie kolumn, a także pasek narzędzi. Tabela przedstawia numery dysków oraz przypisaną literę, etykietę, typ, pojemność, rozmiar wolnego miejsca, rozmiar używanego miejsca, system plików i status każdego woluminu. Pasek narzędzi składa się z ikon umożliwiających wykonywanie czynności **Cofnij**, **Wykonaj ponownie** i **Wykonaj** dotyczących operacji oczekujących (s. 326).

Panel graficzny w dolnej części widoku przedstawia graficzny obraz wszystkich dysków i ich woluminów w postaci prostokątów zawierających podstawowe dane na ich temat (etykieta, litera, rozmiar, status, typ i system plików).

Obie części widoku pokazują także całe nieprzydzielone miejsce na dysku, które można wykorzystać do tworzenia woluminów.

Uruchamianie operacji

Dowolną operację można uruchomić:

- z menu kontekstowego woluminu lub dysku (zarówno w tabeli, jak i w panelu graficznym),
- z menu **Zarządzanie dyskami** konsoli.
- z paska **Operacje** w panelu **Czynności i narzędzia**.

*Należy pamiętać, że lista operacji dostępnych w menu kontekstowym, w menu **Zarządzanie dyskami** i na pasku **Operacje** zależy od wybranego typu woluminu lub dysku. To samo dotyczy także nieprzydzielonego miejsca.*

Wyświetlanie wyników operacji

Wyniki dowolnej operacji na dysku lub woluminie, która została właśnie zaplanowana, są natychmiast wyświetlane w widoku **Zarządzanie dyskami** konsoli. Na przykład po utworzeniu woluminu zostanie on natychmiast wyświetlony w tabeli, a także w formie graficznej w dolnej części widoku. Również wszelkie zmiany woluminów, między innymi zmiana litery lub etykiety woluminu, są natychmiast wyświetlane w widoku.

6.11.5 Operacje na dyskach

Narzędzie Acronis Disk Director Lite umożliwia wykonywanie na dyskach następujących operacji:

- Inicjowanie dysku (s. 312) — inicjowanie nowego sprzętu dodanego do systemu
- Klonowanie dysku podstawowego (s. 312) — przenoszenie kompletnych danych ze źródłowego podstawowego dysku MBR na dysk docelowy
- Konwersja dysków: MBR na GPT (s. 315) — konwertowanie tabeli partycji MBR na GPT
- Konwersja dysków: GPT na MBR (s. 315) — konwertowanie tabeli partycji GPT na MBR

- Konwersja dysków: podstawowy na dynamiczny (s. 316) — konwertowanie dysku podstawowego na dynamiczny
- Konwersja dysków: dynamiczny na podstawowy (s. 317) — konwertowanie dysku dynamicznego na podstawowy

Pełna wersja programu Acronis Disk Director oferuje więcej narzędzi do pracy z dyskami.

Program Acronis Disk Director Lite musi uzyskać wyłączny dostęp do dysku docelowego. Oznacza to, że w tym czasie nie mogą z niego korzystać żadne inne narzędzia do zarządzania dyskami (na przykład narzędzie Windows Disk Management). Po wyświetleniu komunikatu informującego o tym, że nie można zablokować dysku, należy zamknąć aplikacje do zarządzania dyskami używające tego dysku i rozpocząć jeszcze raz. Jeśli nie można ustalić, które aplikacje używają dysku, należy zamknąć je wszystkie.

Inicjowanie dysku

Po dodaniu nowego dysku do komputera narzędzie Acronis Disk Director Lite wykryje zmianę konfiguracji i przeskanuje dodany dysk, aby uwzględnić go na liście dysków i woluminów. Jeśli dysk nie został zainicjowany lub system komputera nie rozpoznaje jego struktury plików, oznacza to, że na dysku tym nie można instalować programów ani przechowywać plików.

Narzędzie Acronis Disk Director Lite wykryje, że dysk nie może być używany przez system i wymaga zainicjowania. W widoku **Zarządzanie dyskami** nowo wykryty sprzęt będzie wyświetlany jako szary blok z wyszarzoną ikoną, co oznacza, że dysk nie może być używany w systemie.

Jeśli konieczna jest inicjalizacja dysku:

1. Wybierz dysk do inicjalizacji.
2. Kliknij prawym przyciskiem myszy wybrany wolumin, a następnie w menu kontekstowym kliknij **Inicjuj**. Zostanie wyświetlone okno **Inicjowanie dysku**, w którym zostaną przedstawione podstawowe informacje o sprzęcie, takie jak numer, pojemność i stan dysku, które mogą pomóc w wybraniu odpowiedniej czynności.
3. Okno to umożliwia wybranie schematu partycjonowania dysku (MBR lub GPT) oraz typu dysku (podstawowy lub dynamiczny). Nowy stan dysku zostanie natychmiast przedstawiony w formie graficznej w widoku **Zarządzanie dyskami**.
4. Po kliknięciu przycisku **OK** zostanie dodana oczekująca operacja inicjacji dysku.

(Aby zakończyć dodawaną operację, należy ją przesłać (s. 326). Wyjście z programu bez wykonania operacji oczekujących spowoduje ich anulowanie).

Po zakończeniu inicjowania całe miejsce na dysku jest nieprzydzielone, a więc nie może być używane do instalowania programów ani przechowywania plików. Aby umożliwić korzystanie z dysku, należy w normalny sposób wykonać operację **Utwórz wolumin**.

Jeśli zechcesz zmienić ustawienia dysku, możesz to zrobić później, używając standardowych funkcji dyskowych dostępnych w narzędziu Acronis Disk Director Lite.

Klonowanie dysku podstawowego

Czasami trzeba przenieść wszystkie dane z dysku na nowy dysk, na przykład podczas powiększania woluminu systemowego, uruchamiania nowego układu systemu lub ratowania dysku ze względu na usterkę sprzętową. W każdym z tych przypadków przyczynę operacji **Klonuj dysk podstawowy** można podsumować jako konieczność przeniesienia wszystkich danych z dysku źródłowego na dysk docelowy w dokładnie takiej samej postaci.

Narzędzie Acronis Disk Director Lite umożliwia wykonywanie tej operacji tylko na podstawowych dyskach MBR.

Aby zaplanować operację **Klonuj dysk podstawowy**:

1. Wybierz dysk do sklonowania.
2. Wybierz dysk docelowy operacji klonowania.
3. Wybierz metodę klonowania i określ opcje zaawansowane.

Nowa struktura woluminów zostanie natychmiast przedstawiona w formie graficznej w widoku **Zarządzanie dyskami**.

*Przed sklonowaniem dysku systemowego zaleca się wyłączenie funkcji Acronis Startup Recovery Manager (s. 418) (ASRM), jeśli jest aktywna. W przeciwnym razie sklonowany system operacyjny może się nie uruchamiać. Po zakończeniu klonowania można z powrotem włączyć funkcję ASRM. Jeśli dezaktywacja jest niemożliwa, należy wybrać metodę klonowania dysku **Tak jak jest**.*

Wybieranie dysku źródłowego i docelowego

Program wyświetla listę dysków podzielonych na partycje. Użytkownik musi wybrać dysk źródłowy, z którego dane zostaną przeniesione na inny dysk.

Kolejnym krokiem jest wybranie dysku docelowego operacji klonowania. Program umożliwia wybranie dysku, jeśli jego rozmiar wystarczy, aby pomieścić wszystkie dane z dysku źródłowego bez żadnych strat.

Jeśli na dysku wybranym jako docelowy znajdują się jakiekolwiek dane, zostanie wyświetlony komunikat: „**Wybrany dysk docelowy nie jest pusty. Dane w jego woluminach zostaną zastąpione.**”. Komunikat ten oznacza, że wszystkie dane, które aktualnie znajdują się na wybranym dysku docelowym, zostaną nieodwołalnie utracone.

Metoda klonowania i opcje zaawansowane

Operacja **Klonuj dysk podstawowy** zazwyczaj oznacza, że informacje z dysku źródłowego są przenoszone na dysk docelowy metodą „**Tak jak jest**”. Jeśli więc dysk docelowy ma taki sam rozmiar (lub jest większy), wszystkie informacje można na niego przenieść dokładnie w takiej postaci, w jakiej są przechowywane na dysku źródłowym.

Jednak w warunkach dużej różnorodności dostępnych urządzeń zazwyczaj dysk docelowy ma inny rozmiar niż dysk źródłowy. Jeśli dysk docelowy jest większy, warto wybrać opcję **Proporcjonalna zmiana rozmiaru woluminu**, która pozwala uniknąć pozostawienia na dysku docelowym nieprzydzielonego miejsca. Opcja **Klonuj dysk podstawowy** „tak jak jest” nie ulega zmianie, ale domyślna metoda klonowania jest wykonywana z proporcjonalnym powiększeniem wszystkich woluminów dysku **źródłowego**, aby na dysku **docelowym** nie pozostało nieprzydzielone miejsce.

Jeśli dysk docelowy jest mniejszy, opcja klonowania **Tak jak jest** jest niedostępna, natomiast konieczna staje się proporcjonalna zmiana rozmiaru woluminów dysku **źródłowego**. Program analizuje dysk **docelowy** w celu ustalenia, czy jego rozmiar wystarczy do pomieszczenia wszystkich danych z dysku **źródłowego** bez żadnych strat. Jeśli przeniesienie z proporcjonalną zmianą rozmiaru woluminów dysku **źródłowego** jest możliwe bez utraty danych, użytkownik może kontynuować. Jeśli ze względu na ograniczenia rozmiaru bezpieczne przeniesienie wszystkich danych z dysku **źródłowego** na dysk **docelowy** jest niemożliwe nawet w przypadku proporcjonalnej zmiany rozmiaru woluminów, wykonanie operacji **Klonuj dysk podstawowy** jest niemożliwe i użytkownik nie może kontynuować.

Jeśli klonowany ma być dysk zawierający **wolumin systemowy**, należy zwrócić uwagę na **Opcje zaawansowane**.

Kliknięcie **Zakończ** spowoduje dodanie oczekującej operacji klonowania dysku.

(Aby zakończyć dodawaną operację, należy ją wykonać (s. 326). Wyjście z programu bez wykonania operacji oczekujących spowoduje ich anulowanie).

Używanie opcji zaawansowanych

W przypadku klonowania dysku zawierającego **wolumin systemowy** trzeba zachować możliwość uruchamiania systemu operacyjnego na woluminie dysku docelowego. Oznacza to, że w systemie operacyjnym informacje o woluminie systemowym (na przykład litera woluminu) muszą pasować do podpisu NT dysku, przechowywanego w jego rekordzie MBR. Ale dwa dyski o tym samym podpisie NT nie mogą działać prawidłowo w jednym systemie operacyjnym.

Jeśli dwa dyski w komputerze mają ten sam podpis NT i zawierają wolumin systemowy, podczas rozruchu system operacyjny uruchamia się z pierwszego dysku, wykrywa taki sam podpis na drugim dysku, automatycznie generuje nowy, unikatowy podpis NT i przypisuje go do drugiego dysku. Skutkiem tego wszystkie woluminy na drugim dysku tracą swoje litery, wszystkie ścieżki na dysku stają się nieprawidłowe, a programy nie mogą znaleźć swoich plików. Uruchomienie systemu operacyjnego umieszczonego na tym dysku jest niemożliwe.

Możliwość uruchamiania systemu na woluminie dysku docelowego można zachować przy użyciu jednej z dwóch opcji:

1. Kopiuj podpis NT — dysk docelowy otrzymuje podpis NT dysku źródłowego pasujący do kluczy rejestru także skopiowanych na dysk docelowy.
2. Pozostaw podpis NT — stary podpis dysku docelowego jest zachowywany, a system operacyjny jest aktualizowany odpowiednio do tego podpisu.

Jeśli trzeba skopiować podpis NT:

1. Zaznacz pole wyboru **Kopiuj podpis NT**. Zostanie wyświetlone ostrzeżenie: „Jeśli na dysku twardym znajduje się system operacyjny, przed ponownym uruchomieniem należy odinstalować źródłowy lub docelowy dysk twardy komputera. W przeciwnym razie system operacyjny zostanie uruchomiony z pierwszego z nich, a systemu operacyjnego znajdującego się na drugim dysku nie będzie można uruchomić”. Pole wyboru **Wyłącz komputer po wykonaniu operacji klonowania** jest zaznaczane i wyłączane automatycznie.
2. Kliknij **Zakończ**, aby dodać operację oczekującą.
3. Kliknij **Wykonaj** na pasku narzędzi, a następnie kliknij **Kontynuuj** w oknie **Operacje oczekujące**.
4. Zaczekaj na zakończenie operacji.
5. Zaczekaj na wyłączenie komputera.
6. Odłącz źródłowy lub docelowy dysk twardy od komputera.
7. Uruchom komputer.

Jeśli trzeba zachować podpis NT:

1. W razie potrzeby kliknij pole wyboru **Kopiuj podpis NT**, aby je wyczyścić.
2. W razie potrzeby kliknij pole wyboru **Wyłącz komputer po wykonaniu operacji klonowania**, aby je wyczyścić.
3. Kliknij **Zakończ**, aby dodać operację oczekującą.
4. Kliknij **Wykonaj** na pasku narzędzi, a następnie kliknij **Kontynuuj** w oknie **Operacje oczekujące**.
5. Zaczekaj na zakończenie operacji.

Konwersja dysków: MBR na GPT

Konwersja podstawowego dysku MBR na podstawowy dysk GPT może być konieczna w następujących przypadkach:

- Jeśli na jednym dysku potrzebnych jest więcej niż 4 woluminy podstawowe.
- Jeśli konieczna jest dodatkowa ochrona przed możliwym uszkodzeniem danych.

Jeśli konieczna jest konwersja podstawowego dysku MBR na podstawowy dysk GPT:

1. Wybierz podstawowy dysk MBR, który ma zostać przekonwertowany na dysk GPT.
2. Kliknij prawym przyciskiem myszy wybrany wolumin, a następnie kliknij **Konwertuj na GPT** w menu kontekstowym.

   Zostanie wyświetlone okno ostrzeżenia informujące o zamierzonym przekonwertowaniu dysku MBR na GPT.
3. Kliknięcie **OK** spowoduje dodanie operacji oczekującej konwersji dysku MBR na GPT.

(Aby zakończyć dodaną operację, należy ją wykonać (s. 326). Wyjście z programu bez wykonania operacji oczekujących spowoduje ich skuteczne anulowanie).

Należy pamiętać, że dysk podzielony na partycje GPT rezerwuje na końcu obszaru partycji miejsce potrzebne na obszar kopii zapasowych, w którym są przechowywane kopie nagłówka GPT i tabeli partycji. Jeśli dysk jest pełny i nie można automatycznie zwiększyć rozmiaru woluminu, operacja konwersji dysku MBR na GPT zakończy się niepowodzeniem.

Operacja jest nieodwracalna. Jeśli wolumin podstawowy należący do dysku MBR zostanie przekonwertowany najpierw na dysk GPT, a następnie z powrotem na dysk MBR, stanie się woluminem logicznym i nie będzie można używać go jako woluminu systemowego.

Jeśli użytkownik planuje zainstalowanie systemu operacyjnego, który nie obsługuje dysków GPT, konwersja wsteczna na dysk MBR jest także możliwa za pośrednictwem tych samych elementów menu. Nazwa operacji będzie wyświetlana jako **Konwertuj na MBR**.

Konwersja dysków dynamicznych: MBR na GPT

Narzędzie Acronis Disk Director Lite nie obsługuje bezpośredniej konwersji dysków dynamicznych MBR na GPT. Jednak ten sam cel można osiągnąć przy użyciu programu, wykonując następujące konwersje:

1. Konwersja dysku MBR: dynamiczny na podstawowy (s. 317) przy użyciu operacji **Konwertuj na podstawowy**.
2. Konwersja dysku podstawowego: MBR na GPT przy użyciu operacji **Konwertuj na GPT**.
3. Konwersja dysku GPT: podstawowy na dynamiczny (s. 316) przy użyciu operacji **Konwertuj na dynamiczny**.

Konwersja dysku: GPT na MBR

Jeśli użytkownik planuje zainstalowanie systemu operacyjnego, który nie obsługuje dysków GPT, można przekonwertować dysk GPT na MBR. Nazwa operacji będzie wyświetlana jako **Konwertuj na MBR**.

Jeśli trzeba przekonwertować dysk GPT na MBR:

1. Wybierz dysk GPT, który ma zostać przekonwertowany na dysk MBR.
2. Kliknij prawym przyciskiem myszy wybrany wolumin, a następnie kliknij **Konwertuj na MBR** w menu kontekstowym.

Zostanie wyświetlone okno ostrzeżenia informujące o zamierzonym przekonwertowaniu dysku GPT na MBR.

Zostaną wyświetlone informacje o zmianach, jakie dokonają się w systemie po przekonwertowaniu wybranego dysku GPT na MBR. Na przykład o tym, że jeśli tego rodzaju konwersja uniemożliwi dostęp systemu do dysku, po przeprowadzeniu konwersji system operacyjny przestanie się ładować lub niektóre woluminy z wybranego dysku GPT będą niedostępne na dysku MBR (np. woluminy znajdujące się w odległości większej niż 2 TB od początku dysku). Zostanie wyświetlone ostrzeżenie o tego rodzaju uszkodzeniach.

Należy pamiętać, że po wykonaniu tej operacji wolumin należący do konwertowanego dysku GPT stanie się woluminem logicznym i jest to nieodwracalne.

3. Kliknięcie **OK** powoduje dodanie operacji oczekującej konwersji dysku GPT na MBR.

(Aby zakończyć dodaną operację, należy ją wykonać (s. 326). Wyjście z programu bez wykonania operacji oczekujących spowoduje ich skuteczne anulowanie).

Konwersja dysku: podstawowy na dynamiczny

Konwersja dysku podstawowego na dynamiczny może być konieczna w następujących przypadkach:

- Dysk ma stanowić część grupy dysku dynamicznego.
- Chodzi o uzyskanie dodatkowej ochrony danych przechowywanych na dysku.

Jeśli trzeba przekonwertować dysk podstawowy na dynamiczny:

1. Wybierz dysk podstawowy, który ma zostać przekonwertowany na dynamiczny.
2. Kliknij prawym przyciskiem myszy wybrany wolumin, a następnie kliknij **Konwertuj na dynamiczny** w menu kontekstowym. Zostanie wyświetlone ostatnie ostrzeżenie o konwersji dysku podstawowego na dynamiczny.
3. Kliknięcie **OK** w tym oknie ostrzeżenia spowoduje natychmiastowe wykonanie konwersji, a w razie potrzeby ponowne uruchomienie komputera.

Uwaga: dysk dynamiczny zajmuje ostatni megabajt dysku fizycznego w celu przechowywania bazy danych zawierającej czteropoziomowy opis każdego woluminu dynamicznego (Wolumin-Komponent-Partycja-Dysk). Jeśli podczas konwersji dysku na dynamiczny okaże się, że dysk podstawowy jest pełny i nie można automatycznie zmniejszyć rozmiaru jego woluminów, operacja konwersji dysku podstawowego na dynamiczny zakończy się niepowodzeniem.

Gdy użytkownik zdecyduje się na konwersję wsteczną dysków dynamicznych na podstawowe, na przykład w celu użycia systemu operacyjnego na komputerze, który nie obsługuje dysków dynamicznych, może przekonwertować dyski przy użyciu tych samych elementów menu, jednak tym razem operacja będzie nosiła nazwę **Konwertuj na podstawowy**.

Konwersja dysku systemowego

Narzędzie Acronis Disk Director Lite nie wymaga ponownego uruchomienia systemu operacyjnego po zakończeniu konwersji dysku podstawowego na dynamiczny, gdy:

1. na dysku jest zainstalowany jeden system operacyjny Windows 2008/Vista;
2. ten system operacyjny jest uruchomiony na komputerze.

Konwersja dysku podstawowego, składającego się z woluminów systemowych, na dysk dynamiczny zajmuje trochę czasu, a każda przerwa w dopływie zasilania, niezamierzone wyłączenie komputera lub przypadkowe naciśnięcie przycisku Reset podczas wykonywania procedury może spowodować utratę możliwości uruchomienia.

W odróżnieniu od Menedżera dysków systemu Windows program zapewnia możliwość uruchomienia **systemu operacyjnego w trybie offline** na dysku po zakończeniu operacji.

Konwersja dysków: dynamiczne na podstawowe

Konwersja dysków dynamicznych na podstawowe może być konieczna na przykład w przypadku, gdy użytkownik chce rozpocząć korzystanie z systemu operacyjnego na komputerze, który nie obsługuje dysków dynamicznych.

Jeśli trzeba wykonać konwersję dysku dynamicznego na podstawowy:

1. Wybierz dysk dynamiczny, który ma zostać przekonwertowany na podstawowy.
2. Kliknij prawym przyciskiem myszy wybrany wolumin, a następnie kliknij **Konwertuj na podstawowy** w menu kontekstowym. Zostanie wyświetlone ostatnie ostrzeżenie o konwersji dysku dynamicznego na podstawowy.

   Zostaną wyświetlone informacje o zmianach, jakie dokonają się w systemie po przekonwertowaniu wybranego dysku dynamicznego na podstawowy, np. o tym, że jeśli tego rodzaju konwersja uniemożliwi dostęp systemu do dysku, po przeprowadzeniu konwersji system operacyjny przestanie się ładować. Jeśli natomiast dysk przeznaczony do konwersji na podstawowy zawiera jakiekolwiek woluminy, których typy są obsługiwane wyłącznie przez dyski dynamiczne (wszystkie typy woluminów, z wyjątkiem woluminów prostych), w tym miejscu zostanie wyświetlone ostrzeżenie o możliwości uszkodzenia konwertowanych danych.

   Należy pamiętać, że operacja jest niedostępna w przypadku dysku dynamicznego zawierającego woluminy łączone, rozłożone lub RAID-5.

3. Kliknięcie **OK** w tym oknie ostrzeżenia spowoduje natychmiastowe wykonanie konwersji.

Po zakończeniu konwersji ostatnie 8 MB miejsca na dysku jest rezerwowane na potrzeby konwersji dysku z podstawowego na dynamiczny w przyszłości.

W niektórych przypadkach możliwe nieprzydzielone miejsce i proponowany maksymalny rozmiar woluminu mogą się różnić (np. gdy rozmiar jednego woluminu lustrzanego ustala rozmiar drugiego lub gdy ostatnie 8 MB miejsca na dysku zostaje zarezerwowane na potrzeby konwersji dysku z podstawowego na dynamiczny w przyszłości).

Konwersja dysku systemowego

w następujących przypadkach narzędzie Acronis Disk Director Lite nie wymaga ponownego uruchomienia systemu operacyjnego po zakończeniu konwersji dysku dynamicznego na podstawowy:

1. Na dysku jest zainstalowany jeden system operacyjny Windows 2008/Vista.
2. Ten system operacyjny jest uruchomiony na komputerze.

Konwersja dysku dynamicznego, składającego się z woluminów systemowych, na dysk podstawowy zajmuje trochę czasu, a każda przerwa w dopływie zasilania, niezamierzone wyłączenie komputera lub przypadkowe naciśnięcie przycisku Reset podczas wykonywania procedury może spowodować utratę możliwości uruchomienia.

W odróżnieniu od Menedżera dysków systemu Windows program zapewnia:

- bezpieczną konwersję dysku dynamicznego na podstawowy, gdy zawiera on woluminy **z danymi** woluminów prostych i lustrzanych;
- na komputerach z funkcją uruchamiania wielu systemów operacyjnych możliwość uruchomienia systemu, który w czasie operacji znajdował się w trybie **offline**.

Zmiana statusu dysku

Zmiana statusu dysku, możliwa w systemach operacyjnych Windows Vista SP1, Windows Server 2008 i Windows 7, ma zastosowanie do bieżącego układu dysku (s. 310).

W widoku graficznym dysku obok jego nazwy zawsze wyświetlany jest jeden z następujących statusów dysku:

- **Online**

  Status online oznacza, że dysk jest dostępny w trybie do odczytu i zapisu. Jest to normalny status dysku. Jeśli dysk ma być dostępny w trybie tylko do odczytu, wybierz dysk i zmień jego status na offline, wybierając **Zmień status dysku na offline** z menu **Operacje**.

- **Offline**

  Status offline oznacza, że dysk jest dostępny w trybie tylko do odczytu. Aby z powrotem ustawić status online dysku, wybierz **Zmień status dysku na online** z menu **Operacje**.
  Jeśli dysk ma status offline i nazwę **Brakujący**, oznacza to, że system operacyjny nie może znaleźć lub rozpoznać dysku. Dysk może być uszkodzony, odłączony lub wyłączony. Aby uzyskać informacje o przywracaniu brakującego dysku o statusie offline do statusu online, zobacz następujący artykuł z bazy wiedzy firmy Microsoft: http://technet.microsoft.com/pl-pl/library/cc732026.aspx.

Importowanie dysków obcych

Na komputerze, na którym znajdują się co najmniej dwa systemy operacyjne, sposób przedstawiania dysków i woluminów zależy od aktualnie uruchomionego systemu operacyjnego.

Zwykle wszystkie dyski dynamiczne utworzone na tym samym komputerze należą do tej samej grupy dysków. Po przeniesieniu do innego komputera lub dodaniu do innego systemu operacyjnego na tym samym komputerze grupa dysków jest uważana za **obcą**. Obcych grup dysków nie można używać, dopóki nie zostaną zaimportowane do istniejącej grupy dysków. Jeśli na komputerze nie ma żadnej grupy dysków, obca grupa dysków jest importowana w stanie „tak jak jest” (z oryginalną nazwą).

Aby uzyskać dostęp do dysków obcych, należy dodać te dyski do konfiguracji systemu przy użyciu operacji **Importuj dyski obce**.

Wszystkie dyski dynamiczne w obcej grupie dysków są importowane jednocześnie. Nie można zaimportować tylko jednego dysku dynamicznego.

Aby zaimportować dyski obce

1. Kliknij prawym przyciskiem myszy dyski obce, a następnie kliknij **Importuj dyski obce**.

   Pojawi się okno zawierające listę wszystkich obcych dysków dynamicznych dodanych do komputera oraz informacje na temat woluminów do zaimportowania. Statusy woluminów umożliwiają określenie, czy są importowane wszystkie wymagane dyski z grupy dysków. Gdy są importowane wszystkie wymagane dyski, ich woluminy będą miały status **W dobrej kondycji**. Status inny niż **W dobrej kondycji** oznacza, że nie zostały zaimportowane wszystkie dyski.

   Więcej informacji na temat statusów woluminów można znaleźć w artykule firmy Microsoft pod adresem: http://technet.microsoft.com/pl-pl/library/cc771775.aspx.

2. Kliknij **OK**, aby dodać oczekującą operację importowania dysków obcych.

Wyniki operacji oczekującej są od razu wyświetlane tak, jakby operacja została zrealizowana.

Aby zrealizować operację oczekującą, należy ją wykonać. Zamknięcie programu bez wykonania operacji oczekujących powoduje ich anulowanie.

6.11.6 Operacje w woluminach

Narzędzie Acronis Disk Director Lite umożliwia wykonywanie następujących operacji na woluminach:

- Utwórz wolumin (s. 319) — tworzy nowy wolumin z pomocą Kreatora tworzenia woluminów.
- Usuń wolumin (s. 323) — usuwa wybrany wolumin.
- Set Active (s. 323) (Ustaw jako aktywny) — ustawia wybrany wolumin jako aktywny, aby umożliwić uruchamianie komputera z zainstalowanym w tym woluminie systemem operacyjnym.
- Zmień literę (s. 324) — zmienia literę wybranego woluminu.
- Zmień etykietę (s. 324) — zmienia etykietę wybranego woluminu.
- Formatowanie woluminu (s. 325) — formatuje wolumin, zapewniając mu niezbędny system plików.

Pełna wersja programu Acronis Disk Director oferuje więcej narzędzi do pracy z woluminami.

Program Acronis Disk Director Lite musi uzyskać wyłączny dostęp do woluminu docelowego. Oznacza to, że w tym czasie nie mogą z niego korzystać żadne inne narzędzia do zarządzania dyskami (na przykład narzędzie Windows Disk Management). Po wyświetleniu komunikatu informującego o tym, że nie można zablokować woluminu, należy zamknąć aplikacje do zarządzania dyskami używające tego woluminu i rozpocząć jeszcze raz. Jeśli nie można ustalić, które aplikacje używają woluminu, należy zamknąć je wszystkie.

Tworzenie woluminu

Nowy wolumin może być potrzebny do:

- odzyskania zapisanej wcześniej kopii zapasowej w konfiguracji „dokładnie tak, jak był”;
- oddzielnego przechowywania kolekcji podobnych plików, na przykład kolekcji MP3 lub plików wideo w oddzielnym woluminie;
- przechowywania kopii zapasowych (obrazów) innych woluminów/dysków w woluminie specjalnym;
- zainstalowania nowego systemu operacyjnego (lub pliku wymiany) w nowym woluminie;
- dodania nowego sprzętu do komputera.

W programie Acronis Disk Director Lite do tworzenia woluminów służy **Kreator tworzenia woluminów**.

Typy woluminów dynamicznych

Wolumin prosty

Wolumin utworzony z wolnego miejsca na pojedynczym dysku fizycznym. Może składać się z jednego regionu na dysku lub z kilku regionów połączonych wirtualnie przez Menedżera dysków logicznych (LDM). Nie zapewnia większej niezawodności, większej szybkości ani dodatkowego miejsca.

Wolumin łączony

Wolumin utworzony z wolnego miejsca na kilku dyskach fizycznych, połączony wirtualnie przez LDM. Jeden wolumin może obejmować maksymalnie 32 dyski, co pozwala na pokonanie sprzętowych ograniczeń rozmiaru, ale awaria jednego dysku spowoduje utratę wszystkich danych. Nie można również usunąć żadnej części woluminu łączonego, nie niszcząc całego

woluminu. Dlatego wolumin łączony nie zapewnia większej niezawodności ani większej szybkości wykonywania operacji wejścia/wyjścia.

Wolumin rozłożony

Wolumin (nazywany czasami RAID 0) składający się z równych fragmentów danych rozłożonych między poszczególne dyski w woluminie. Oznacza to, że do utworzenia woluminu rozłożonego użytkownik potrzebuje dwóch lub więcej dysków dynamicznych. Dyski w woluminie rozłożonym nie muszą być identyczne, ale na każdym dysku, który ma zostać uwzględniony w woluminie, musi być dostępne nieużywane miejsce, a rozmiar woluminu będzie zależał od rozmiaru najmniejszego miejsca. Dostęp do danych w woluminie rozłożonym jest zazwyczaj szybszy niż do tych samych danych na pojedynczym dysku fizycznym, ponieważ operacje wejścia/wyjścia są rozłożone na kilka dysków.

Woluminy rozłożone tworzy się w celu zwiększenia wydajności, a nie ze względu na większą niezawodność — nie zawierają one nadmiarowych informacji.

Wolumin lustrzany

Wolumin odporny na uszkodzenia (nazywany czasami RAID 1), którego dane są zduplikowane na dwóch identycznych dyskach fizycznych. Wszystkie dane z jednego dysku są kopiowane na drugi dysk w celu zapewnienia nadmiarowości danych. Woluminem lustrzanym może być prawie każdy wolumin, w tym również systemowy i startowy. Jeśli jeden dysk ulegnie uszkodzeniu, dane wciąż będą dostępne na pozostałych dyskach. Niestety, w przypadku korzystania z woluminów lustrzanych sprzętowe ograniczenia rozmiaru i wydajności są jeszcze większe.

Wolumin lustrzany-rozłożony

Wolumin odporny na uszkodzenia (nazywany czasami RAID 1+0), łączący w sobie zalety dużej szybkości operacji wejścia wyjścia w układzie rozłożonym z nadmiarowością, jaką zapewnia typ lustrzany. Oczywistą wadą wynikającą z architektury lustrzanej jest niski współczynnik rozmiaru dysku do rozmiaru woluminu.

RAID-5

Wolumin odporny na uszkodzenia, którego dane rozkładają się na trzy lub więcej dysków. Dyski nie muszą być identyczne, ale na każdym dysku w woluminie muszą być dostępne równej wielkości bloki nieprzydzielonego miejsca. Także parzystość (obliczona wartość, która może zostać użyta do rekonstrukcji danych w przypadku uszkodzenia) jest rozłożona na całej macierzy dyskowej. Ponadto jest ona zawsze przechowywana na innym dysku niż same dane. W przypadku awarii dysku fizycznego część woluminu RAID-5 znajdująca się na uszkodzonym dysku może zostać odtworzona na podstawie pozostałych danych i parzystości. Wolumin RAID-5 zapewnia niezawodność i umożliwia przekroczenie ograniczeń związanych z rozmiarem dysku fizycznego dzięki wyższemu wskaźnikowi dysk lustrzany/rozmiar woluminu.

Kreator tworzenia woluminów

Kreator tworzenia woluminów pozwala na utworzenie dowolnego typu woluminu (w tym również systemowego i aktywnego), wybranie systemu plików, opatrzenie etykietą, przypisanie litery. Zawiera także inne funkcje zarządzania dyskami.

Na jego stronach można wprowadzać parametry operacji, wykonywać kolejne operacje, a w razie potrzeby wracać do poprzednich czynności w celu zmiany dowolnych wybranych wcześniej opcji. W dokonaniu wyboru pomagają szczegółowe instrukcje dotyczące poszczególnych parametrów.

Aby utworzyć wolumin:

Należy uruchomić **Kreator tworzenia woluminów**, wybierając **Utwórz wolumin** na pasku **Kreatory**, lub kliknąć prawym przyciskiem myszy dowolne nieprzydzielone miejsce i wybrać **Utwórz wolumin** w wyświetlonym menu kontekstowym.

Wybierz typ tworzonego woluminu

Najpierw należy określić typ woluminu, który ma zostać utworzony. Dostępne są następujące typy woluminów:

- Podstawowy
- Prosty/łączony
- Rozłożony
- Lustrzany
- RAID-5

Każda możliwa architektura woluminów zostanie opatrzona krótkim opisem, co umożliwia lepsze zrozumienie jej zalet i ograniczeń.

*Jeśli bieżący system operacyjny zainstalowany na tym komputerze nie obsługuje wybranego typu woluminu, zostanie wyświetlone odpowiednie ostrzeżenie. W takim przypadku przycisk **Dalej** będzie wyłączony i trzeba będzie wybrać inny typ woluminu, aby kontynuować tworzenie nowego woluminu.*

Po kliknięciu przycisku **Dalej** nastąpi przejście do strony kreatora: Wybierz dyski docelowe (s. 321).

Wybierz dyski docelowe

Na następnej stronie kreatora zostanie wyświetlony monit o wybranie dysków z miejscem do tworzenia woluminu.

Aby utworzyć wolumin podstawowy:

- Wybierz dysk docelowy i określ nieprzydzielone miejsce, aby utworzyć w nim wolumin podstawowy.

Aby utworzyć wolumin prosty/łączony:

- Wybierz jeden lub więcej dysków docelowych, aby utworzyć na nich wolumin.

Aby utworzyć wolumin lustrzany:

- Wybierz dwa dyski docelowe, na których zostanie utworzony wolumin.

Aby utworzyć wolumin rozłożony:

- Wybierz dwa lub więcej dysków docelowych, aby utworzyć na nich wolumin.

Aby utworzyć wolumin RAID-5:

- Wybierz trzy dyski docelowe, na których zostanie utworzony wolumin.

Po wybraniu dysków kreator obliczy maksymalny rozmiar woluminu wynikowego w zależności od rozmiaru nieprzydzielonego miejsca na wybranych dyskach oraz wymagań wybranego wcześniej typu woluminu.

Jeśli użytkownik tworzy wolumin **dynamiczny** i jako miejsce docelowe wybierze jeden lub kilka dysków **podstawowych**, zostanie wyświetlone ostrzeżenie, że wybrany dysk zostanie automatycznie przekonwertowany na dynamiczny.

W razie potrzeby zostanie wyświetlony monit o dodanie niezbędnej liczby dysków, zgodnie z wybranym typem przyszłego woluminu.

Kliknięcie przycisku **Wstecz** spowoduje powrót do strony: Wybierz typ tworzonego woluminu (s. 321).

Kliknięcie przycisku **Dalej** spowoduje przejście do strony: Ustaw rozmiar woluminu (s. 322).

Ustaw rozmiar woluminu

Na trzeciej stronie kreatora można określić rozmiar przyszłego woluminu, zgodnie z wybranymi wcześniej opcjami. W celu wybrania niezbędnego rozmiaru z zakresu od wartości minimalnej do wartości maksymalnej należy użyć suwaka, wprowadzić potrzebne wartości w specjalnych oknach lub kliknąć specjalny uchwyt, a następnie przytrzymać i przeciągnąć granice obrazu dysku za pomocą kursora.

Wartość maksymalna zazwyczaj obejmuje największe możliwe nieprzydzielone miejsce. Jednak w niektórych przypadkach możliwe nieprzydzielone miejsce i proponowany maksymalny rozmiar woluminu mogą się różnić (np. gdy rozmiar jednego woluminu lustrzanego ustala rozmiar drugiego lub gdy 8 MB miejsca na dysku zostaje zarezerwowane na potrzeby konwersji dysku z podstawowego na dynamiczny w przyszłości).

W przypadku woluminów podstawowych pozostawienie na dysku pewnej ilości nieprzydzielonego miejsca umożliwi także wybranie położenia nowego woluminu na dysku.

Kliknięcie przycisku **Wstecz** spowoduje powrót do strony: Wybierz dyski docelowe (s. 321).

Kliknięcie przycisku **Dalej** spowoduje przejście do strony: Ustaw opcje woluminu (s. 322).

Ustaw opcje woluminu

Na następnej stronie kreatora można przypisać **literę** woluminu (domyślnie jest to pierwsza wolna litera alfabetu) oraz opcjonalnie jego **etykietę** (domyślnie brak). W tym miejscu można także określić **system plików** i **rozmiar klastra**.

Kreator wyświetli monit o wybranie jednego z systemów plików systemu Windows: FAT16 (wyłączony, gdy ustawiono rozmiar woluminu większy niż 2 GB), FAT32 (wyłączony, gdy ustawiono rozmiar woluminu większy niż 32 GB) lub NTFS. Można także zostawić wolumin **niesformatowany**.

Ustawiając rozmiar klastra, można wybrać dowolną liczbę spośród wstępnie ustawionych wartości dla każdego systemu plików. Należy pamiętać, że program proponuje rozmiar klastra najlepiej dopasowany do woluminu z wybranym systemem plików.

Jeśli użytkownik tworzy wolumin podstawowy, który może być woluminem systemowym, ta strona wygląda inaczej, ponieważ umożliwia wybranie **typu** woluminu — **podstawowego** (**aktywnego podstawowego**) lub **logicznego**.

Zazwyczaj typ **Podstawowy** wybiera się, aby zainstalować w woluminie system operacyjny. Wartość **Aktywny** (domyślnie) należy wybrać, aby zainstalować w tym woluminie system operacyjny, który będzie uruchamiany podczas rozruchu komputera. Jeśli nie zostanie wybrany przycisk **Podstawowy**, opcja **Aktywny** będzie wyłączona. Jeśli wolumin ma służyć do magazynowania danych, należy wybrać opcję **Logiczny**.

---

*Dysk podstawowy może zawierać maksymalnie cztery woluminy podstawowe. Jeśli woluminy już istnieją, dysk trzeba przekonwertować na dynamiczny, w przeciwnym razie opcje **Aktywny** i **Podstawowy** będą wyłączone i*

*będzie można wybrać wyłącznie typ woluminu **Logiczny**. Komunikat ostrzegawczy poinformuje, że nie będzie można uruchomić systemu operacyjnego zainstalowanego w tym woluminie.*

*Jeśli do ustawiania etykiety nowego woluminu będą używane znaki, które nie są obsługiwane przez aktualnie zainstalowany system operacyjny, zostanie wyświetlone odpowiednie ostrzeżenie, a przycisk **Dalej** będzie wyłączony. Aby kontynuować tworzenie nowego woluminu, należy zmienić etykietę.*

Kliknięcie przycisku **Wstecz** spowoduje powrót do strony: Ustaw rozmiar woluminu (s. 322).

Kliknięcie przycisku **Zakończ** spowoduje zakończenie planowania operacji.

Aby wykonać zaplanowaną operację, należy kliknąć **Wykonaj** na pasku narzędzi, a następnie kliknąć **Kontynuuj** w oknie **Operacje oczekujące.**

W przypadku ustawienia rozmiaru klastra 64 KB w systemie FAT16/FAT32 lub 8 KB–64 KB w systemie NTFS system Windows będzie mógł zamontować wolumin, ale niektóre programy (np. programy instalacyjne) mogą niepoprawnie obliczać miejsce na dysku.

Usuń wolumin

Ta wersja programu Acronis Disk Director Lite ma ograniczoną funkcjonalność, ponieważ głównym zadaniem tego narzędzia jest przygotowywanie systemów odzyskanych po awarii do odzyskiwania zapisanych wcześniej obrazów woluminów. Funkcje zmiany rozmiaru istniejących woluminów i tworzenia nowych woluminów przy użyciu wolnego miejsca w istniejących woluminach są dostępne w pełnej wersji oprogramowania, dlatego w tej wersji usunięcie istniejącego woluminu czasami może być jedynym sposobem zwolnienia potrzebnego miejsca na dysku bez zmiany istniejącej konfiguracji dysków.

Po usunięciu woluminu jego miejsce jest dodawane do nieprzydzielonego miejsca na dysku. Można go użyć do utworzenia nowego woluminu lub do zmiany typu innego woluminu.

Aby usunąć wolumin:

1. Wybierz dysk twardy i wolumin do usunięcia.
2. Wybierz **Usuń wolumin** lub podobny element na liście paska bocznego **Operacje** bądź kliknij ikonę **Usuń wybrany wolumin** na pasku narzędzi.

   Jeśli wolumin zawiera jakiekolwiek dane, zostanie wyświetlone ostrzeżenie, że wszystkie informacje w tym woluminie zostaną nieodwracalnie utracone.
3. Kliknięcie **OK** w oknie **Usuń wolumin** powoduje dodanie operacji oczekującej usuwania woluminu.

(Aby zakończyć dodaną operację, należy ją wykonać (s. 326). Wyjście z programu bez wykonania operacji oczekujących spowoduje ich skuteczne anulowanie).

Ustaw aktywny wolumin

Jeśli istnieje kilka woluminów podstawowych, należy określić jeden, który będzie woluminem startowym. W tym celu można ustawić wolumin, który stanie się woluminem aktywnym. Na dysku może znajdować się tylko jeden wolumin aktywny, dlatego jeśli wolumin zostanie ustawiony jako aktywny, wolumin, który był aktywny poprzednio, automatycznie przestanie być woluminem aktywnym.

Jeśli trzeba ustawić wolumin jako aktywny:

1. Wybierz wolumin podstawowy na podstawowym dysku MBR, aby ustawić go jako aktywny.

2. Kliknij prawym przyciskiem myszy wybrany wolumin, a następnie kliknij **Oznacz jako aktywną** w menu kontekstowym.

   Jeśli w systemie nie ma żadnego innego woluminu aktywnego, zostanie dodana operacja oczekująca ustawiania woluminu aktywnego.

   Należy pamiętać, że w wyniku ustawienia nowego woluminu aktywnego może się zmienić litera poprzedniego woluminu aktywnego, co przez co uruchamianie niektórych zainstalowanych programów może być niemożliwe.

3. Jeśli w systemie znajduje się inny wolumin aktywny, najpierw zostanie wyświetlone ostrzeżenie, że poprzedni wolumin aktywny został ustawiony jako pasywny. Kliknięcie **OK** w oknie **Ostrzeżenie** powoduje dodanie operacji oczekującej ustawiania woluminu aktywnego.

   Należy pamiętać, że nawet jeśli w nowym woluminie aktywnym znajduje się system operacyjny, w niektórych przypadkach nie można uruchomić komputera za jego pomocą. Decyzję o ustawieniu nowego woluminu jako aktywnego trzeba potwierdzić.

(Aby zakończyć dodaną operację, należy ją wykonać (s. 326). Wyjście z programu bez wykonania operacji oczekujących spowoduje ich skuteczne anulowanie).

Nowa struktura woluminów zostanie natychmiast przedstawiona w formie graficznej w widoku **Zarządzanie dyskami**.

Zmień literę woluminu

Systemy operacyjne Windows przypisują litery (C:, D: itd.) do woluminów dysku twardego przy uruchamianiu. Litery te są używane przez aplikacje i systemy operacyjne do znajdowania plików i folderów w woluminach.

Podłączenie dodatkowego dysku oraz utworzenie lub usunięcie woluminu na istniejących dyskach może spowodować zmianę konfiguracji systemu. W rezultacie niektóre aplikacje mogą przestać działać prawidłowo. Także automatyczne znajdowanie i otwieranie plików użytkownika może okazać się niemożliwe. Aby temu zapobiec, można ręcznie zmienić litery, które zostały automatycznie przypisane do woluminów przez system operacyjny.

Jeśli trzeba zmienić literę przypisaną do woluminu przez system operacyjny:

1. Wybierz wolumin do zmiany litery.
2. Kliknij prawym przyciskiem myszy wybrany wolumin, a następnie kliknij **Zmień literę** w menu kontekstowym.
3. Wybierz nową literę w oknie **Zmień literę**.
4. Kliknięcie **OK** w oknie **Zmień literę** powoduje dodanie operacji oczekującej przypisywania litery woluminu.

   (Aby zakończyć dodaną operację, należy ją wykonać (s. 326). Wyjście z programu bez wykonania operacji oczekujących spowoduje ich skuteczne anulowanie).

Nowa struktura woluminów zostanie natychmiast przedstawiona w formie graficznej w widoku **Zarządzanie dyskami**.

Zmień etykietę woluminu

Etykieta woluminu to atrybut opcjonalny. Jest to nazwa przypisana do woluminu, która ułatwia jego rozpoznawanie. Na przykład wolumin może mieć nazwę SYSTEM (wolumin z systemem operacyjnym), PROGRAM (wolumin aplikacji), DANE (wolumin danych) itp., ale to nie oznacza, że w takim woluminie można magazynować wyłącznie dane typu podanego na etykiecie.

W systemie Windows etykiety woluminów są pokazywane w drzewie dysków i folderów Eksploratora: WIN98(C:), WINXP(D:), DANE(E:) itp. WIN98, WINXP i DANE to etykiety woluminów. Etykieta woluminu jest pokazywana we wszystkich oknach dialogowych aplikacji umożliwiających otwieranie i zapisywanie plików.

Jeśli trzeba zmienić etykietę woluminu:

1. Kliknij prawym przyciskiem myszy wybrany wolumin, a następnie kliknij **Zmień etykietę**.
2. Wprowadź nową etykietę w polu tekstowym okna **Zmień etykietę**.
3. Kliknięcie **OK** w oknie **Zmień etykietę** powoduje dodanie operacji oczekującej zmiany etykiety woluminu.

   *Jeśli do ustawiania etykiety nowego woluminu będą używane znaki, które nie są obsługiwane przez aktualnie zainstalowany system operacyjny, zostanie wyświetlone odpowiednie ostrzeżenie, a przycisk **OK** będzie wyłączony. Aby kontynuować zmienianie etykiety woluminu, należy używać wyłącznie obsługiwanych znaków.*

   (Aby zakończyć dodaną operację, należy ją wykonać (s. 326). Wyjście z programu bez wykonania operacji oczekujących spowoduje ich skuteczne anulowanie).

Nowa etykieta zostanie natychmiast przedstawiona w formie graficznej w widoku **Zarządzanie dyskami** konsoli.

Formatowanie woluminu

Wolumin można sformatować, aby zmienić jego system plików:

- w celu zaoszczędzenia dodatkowego miejsca, które jest tracone z powodu rozmiaru klastra w systemach plików FAT16 i FAT32;
- w celu szybkiego i dość skutecznego zniszczenia danych znajdujących się w tym woluminie.

Aby sformatować wolumin:

1. Wybierz wolumin do sformatowania.
2. Kliknij prawym przyciskiem myszy wybrany wolumin, a następnie kliknij **Formatuj** w menu kontekstowym.

   Zostanie otwarte okno **Formatowanie woluminu**, w którym można ustawić opcje nowego systemu plików. Do wyboru jest jeden z systemów plików systemu Windows: FAT16 (wyłączony, gdy rozmiar woluminu jest większy niż 2 GB), FAT32 (wyłączony, gdy rozmiar woluminu jest większy niż 32 GB) lub NTFS.

   W razie potrzeby w oknie tekstowym można wprowadzić etykietę woluminu. Domyślnie to okno jest puste.

   Ustawiając rozmiar klastra, można wybrać dowolną liczbę spośród wstępnie ustawionych wartości dla każdego systemu plików. Należy pamiętać, że program proponuje rozmiar klastra najlepiej dopasowany do woluminu z wybranym systemem plików.
3. Kliknięcie **OK** w celu kontynuowania operacji **Formatowanie woluminu** powoduje dodanie operacji oczekującej formatowania woluminu.

   (Aby zakończyć dodaną operację, należy ją wykonać (s. 326). Wyjście z programu bez wykonania operacji oczekujących spowoduje ich skuteczne anulowanie).

Nowa struktura woluminów zostanie przedstawiona w formie graficznej w widoku **Zarządzanie dyskami**.

W przypadku ustawienia rozmiaru klastra 64 KB w systemie FAT16/FAT32 lub 8 KB–64 KB w systemie NTFS system Windows będzie mógł zamontować wolumin, ale niektóre programy (np. programy instalacyjne) mogą niepoprawnie obliczać miejsce na dysku.

6.11.7 Operacje oczekujące

Wszystkie operacje, które zostały przygotowane przez użytkownika w trybie ręcznym lub za pomocą kreatora, są uważane za oczekujące, dopóki użytkownik nie wyda określonego polecenia powodującego trwałe wprowadzenie zmian. Do tego czasu narzędzie Acronis Disk Director Lite prezentuje jedynie nową strukturę woluminów, która powstanie w wyniku wykonania operacji zaplanowanych na dyskach i woluminach. Ta metoda umożliwia kontrolę wszystkich zaplanowanych operacji, ponowne sprawdzenie zamierzonych zmian, a w razie potrzeby anulowanie operacji przed ich wykonaniem.

Aby zapobiec wprowadzeniu jakiejkolwiek niezamierzonej zmiany na dysku, program najpierw wyświetli listę wszystkich operacji oczekujących.

W widoku **Zarządzanie dyskami** znajduje się pasek narzędzi z ikonami umożliwiającymi wykonywanie czynności **Cofnij**, **Wykonaj ponownie** i **Wykonaj** dotyczących operacji oczekujących. Czynności te można także wykonywać z menu **Zarządzanie dyskami** konsoli.

Wszystkie zaplanowane operacje są dodawane do listy operacji oczekujących.

Czynność **Cofnij** umożliwia cofnięcie ostatniej operacji na liście. Ta czynność jest dostępna, dopóki lista nie jest pusta.

Czynność **Wykonaj ponownie** umożliwia przywrócenie ostatniej operacji oczekującej, która została cofnięta.

Czynność **Wykonaj** powoduje otwarcie okna **Operacje oczekujące**, w którym można wyświetlić listę tych operacji. Kliknięcie **Kontynuuj** spowoduje ich wykonanie. Po wybraniu operacji **Kontynuuj** nie można cofnąć żadnych czynności ani operacji. Klikając **Anuluj**, można także anulować zamiar wykonania operacji. Dzięki temu na liście operacji oczekujących nie zostaną wprowadzone żadne zmiany.

Zamknięcie narzędzia Acronis Disk Director Lite bez wykonania operacji oczekujących oznacza ich skuteczne anulowanie, dlatego próba zamknięcia widoku **Zarządzanie dyskami** bez wykonania operacji oczekujących powoduje wyświetlenie odpowiedniego ostrzeżenia.

6.12 Zbieranie informacji o systemie

Narzędzie do zbierania informacji o systemie pozwala zebrać informacje o komputerze, do którego podłączona jest konsola zarządzania, a następnie zapisać je do pliku. Plikiem tym warto dysponować podczas kontaktu z działem pomocy technicznej firmy Acronis.

Ta opcja jest dostępna na nośniku startowym oraz na komputerach, na których zainstalowano agenta dla systemu Windows lub Linux albo serwer Acronis Backup & Recovery 10 Management Server.

Aby zebrać informacje o systemie

1. W konsoli zarządzania wybierz w górnym menu kolejno **Pomoc** > **Zbierz informacje o systemie z** „nazwa komputera”.
2. Określ plik, do którego chcesz zapisać informacje o systemie.

7 Zarządzanie scentralizowane

W tej sekcji opisano operacje, które można wykonać centralnie przy użyciu składników do zarządzania scentralizowanego. Zawartość niniejszej sekcji dotyczy wyłącznie zaawansowanych wersji programu Acronis Backup & Recovery 10.

7.1 Administrowanie serwerem Acronis Backup & Recovery 10 Management Server

W tej sekcji opisano widoki dostępne za pośrednictwem drzewa nawigacji konsoli podłączonej do serwera zarządzania oraz wyjaśniono sposób pracy z każdym widokiem.

7.1.1 Pulpit nawigacyjny

Pulpit nawigacyjny służy do szybkiego szacowania kondycji ochrony danych na zarejestrowanych komputerach. Pulpit nawigacyjny wyświetla podsumowanie działań agentów programu Acronis Backup & Recovery 10, pozwala także sprawdzać wolne miejsce dostępne w skarbcach zarządzanych oraz błyskawicznie identyfikować i rozwiązywać dowolne problemy.

Alerty

Sekcja alertów skupia się na problemach, które wystąpiły na serwerze zarządzania i zarejestrowanych komputerach oraz w skarbcach centralnych, a także oferuje sposoby ich naprawiania i sprawdzania. Najpoważniejsze problemy są wyświetlane u góry. Jeśli w danej chwili nie ma żadnych alertów ani ostrzeżeń, system wyświetla komunikat „No alerts or warnings” (Brak alertów i ostrzeżeń).

Typy alertów

W poniższej tabeli przedstawiono typy komunikatów, które mogą wystąpić.

	Opis	Oferowane działanie	Komentarz
	Zadania zakończone niepowodzeniem: *X*	Wyświetl zadania	Wybranie działania **Wyświetl zadania** spowoduje otwarcie widoku **Plany i zadania tworzenia kopii zapasowych** z zadaniami zakończonymi niepowodzeniem, gdzie można sprawdzić przyczynę niepowodzenia.
	Zadania wymagające działania: *X*	Rozpoznaj...	Jeśli co najmniej jedno zadanie w bazie danych serwera zarządzania wymaga działania użytkownika, na Pulpicie nawigacyjnym widoczny jest alert. Kliknij **Rozpoznaj**, aby otworzyć okno **Zadania wymagające działania użytkownika**, gdzie można sprawdzić wszystkie wystąpienia i określić podjęte decyzje.
	Nie powiodło się sprawdzenie licencji na *X* komputerach	Wyświetl dziennik	Agent Acronis Backup & Recovery 10 łączy się z serwerem Acronis License Server po uruchomieniu, a następnie co 1–5 dni, zgodnie z ustawieniami parametrów konfiguracji agenta. Alert jest wyświetlany w przypadku niepomyślnego sprawdzenia licencji dla co najmniej jednego agenta. Może to nastąpić, gdy serwer licencji był niedostępny lub dane klucza licencji zostały uszkodzone. Aby

			poznać przyczynę niepomyślnego sprawdzenia, kliknij **Wyświetl dziennik**. Jeśli sprawdzenie licencji nie powiedzie się przez okres od 1 do 60 dni (określony w parametrach konfiguracji agenta), działanie agenta zostanie wstrzymane do momentu pomyślnego sprawdzenia licencji.
⚠	Skarbce z małą ilością wolnego miejsca: *X*	Wyświetl skarbce	Ten alert jest wyświetlany, gdy co najmniej jeden skarbiec centralny ma mniej niż 10% wolnego miejsca. Opcja **Wyświetl skarbce** powoduje otwarcie widoku **Skarbce centralne (s. 146),** gdzie można sprawdzić rozmiar skarbca oraz ilość wolnego miejsca i wykonać niezbędne działania w celu zwiększenia ilości wolnego miejsca.
⚠	Nie utworzono nośnika startowego	Utwórz teraz	Aby mieć możliwość odzyskania system operacyjny po niepomyślnym uruchomieniu komputera, należy: 1. Utworzyć kopię zapasową woluminu systemowego (i woluminu startowego, jeśli jest inny) 2. Utworzyć co najmniej jeden nośnik startowy (s. 424). Wybranie działania **Utwórz teraz** spowoduje uruchomienie Generatora nośnika startowego (s. 422).
⚠	Nie utworzono kopii zapasowych od *X* dni na *Y* komputerach	Pokaż listę	Na pulpicie nawigacyjnym pojawia się ostrzeżenie, że na kilku zarejestrowanych komputerach od pewnego czasu nie została utworzona kopia zapasowa danych. Aby skonfigurować czas uznawany za krytyczny, wybierz kolejno: **Opcje > Opcje konsoli > Alerty związane z czasem**.
⚠	Brak połączenia z serwerem zarządzania od *X* dni: *Y* komputerów	Wyświetl komputery	Na pulpicie nawigacyjnym pojawia się ostrzeżenie, że kilka zarejestrowanych komputerów od pewnego czasu nie nawiązało połączenia z serwerem zarządzania, co oznacza, że te komputery mogą nie być centralnie zarządzane. Kliknij **Wyświetl komputery**, aby otworzyć widok **Komputery** z listą komputerów przefiltrowaną według pola „Ostatnie połączenie”. Aby skonfigurować czas uznawany za krytyczny, wybierz kolejno: **Opcje > Opcje konsoli > Alerty związane z czasem**.
⚠	Agent nie jest zainstalowany na serwerze Acronis Backup & Recovery 10 Management Server. Zaleca się utworzenie kopii zapasowej serwera zarządzania w celu ochrony jego konfiguracji.	Zainstaluj komponenty Acronis	Zainstaluj Agenta Acronis Backup & Recovery 10 dla systemu Windows, aby utworzyć kopię zapasową komputera, na którym jest zainstalowany serwer Acronis Backup & Recovery 10 Management Server. Kliknij **Install now** (Zainstaluj teraz), aby uruchomić nowy kreator instalacji.
⚠	Kopia zapasowa serwera Acronis Backup & Recovery 10	Utwórz kopię zapasową	Alert jest wyświetlany tylko, gdy na serwerze zarządzania jest zainstalowany Agent Acronis Backup

	Management Server nie została utworzona od *X* dni		& Recovery 10 dla systemu Windows. Alert ostrzega, że od pewnego czasu nie została utworzona kopia zapasowa danych na serwerze zarządzania. Wybranie działania **Utwórz kopię zapasową** spowoduje wyświetlenie strony **Utwórz plan tworzenia kopii zapasowych**, gdzie można szybko skonfigurować i uruchomić operację utworzenia kopii zapasowej. Aby skonfigurować czas uznawany za krytyczny, wybierz kolejno: **Opcje > Opcje konsoli > Alerty związane z czasem**.

Działania

Na skumulowanym wykresie kolumnowym można przeglądać dzienną historię działań agentów programu Acronis Backup & Recovery 10. Historia jest oparta na wpisach dziennika zebranych z zarejestrowanych komputerów i serwera zarządzania. Na wykresie jest pokazywana liczba wpisów dziennika każdego typu (błąd, ostrzeżenie, informacja) dotyczących konkretnego dnia.

Z prawej strony wykresu są wyświetlane statystyki dotyczące wybranej daty. Wszystkie pola statystyk są interaktywne, tzn. kliknięcie dowolnego pola powoduje otwarcie widoku **Dziennik** z wpisami wstępnie odfiltrowanymi przez to pole.

U góry wykresu można wybrać działania, które będą wyświetlane w zależności od obecności i wagi błędów.

Łącze **Select current date** (Wybierz bieżącą datę) koncentruje wybór na bieżącej dacie.

Widok systemu

Sekcja **Widok systemu** przedstawia podsumowane statystyki zarejestrowanych komputerów, zadań, zasad tworzenia kopii zapasowych i scentralizowanych planów tworzenia kopii zapasowych. Aby uzyskać odpowiednie informacje, należy kliknąć elementy w tych sekcjach (oprócz scentralizowanych planów tworzenia kopii zapasowych). Spowoduje to wyświetlenie odpowiedniego widoku zawierającego odfiltrowane wstępnie komputery, zadania lub zasady tworzenia kopii zapasowych. Na przykład kliknięcie elementu **Bezczynne** w sekcji **Zadania** spowoduje otwarcie widoku **Zadania** zawierającego zadania odfiltrowane według stanu **Bezczynne**.

Informacje prezentowane w sekcji **Widok systemu** są odświeżane po każdej synchronizacji serwera zarządzania z komputerami. Informacje w pozostałych sekcjach są odświeżane co 10 min i po każdym dostępie do pulpitu nawigacyjnego.

Skarbce

W sekcji **Skarbce** są wyświetlane informacje o centralnych skarbcach zarządzanych. Skarbce można sortować według nazw lub według używanego miejsca. W niektórych przypadkach informacje dotyczące wolnego miejsca w skarbcu mogą być niedostępne, na przykład gdy skarbiec znajduje się w bibliotece taśm. Jeśli sam skarbiec jest niedostępny (offline), będzie wyświetlany komunikat „Vault is not available” (Skarbiec jest niedostępny).

7.1.2 Zasady tworzenia kopii zapasowych

Aby umożliwić ochronę wielu komputerów i zarządzanie nimi jako całością, można utworzyć szablon planu tworzenia kopii zapasowych nazywany „zasadami tworzenia kopii zapasowych”. Zastosowanie tego szablonu do grupy komputerów umożliwi wdrożenie wielu planów tworzenia kopii zapasowych

za pomocą jednej czynności. Zasady tworzenia kopii zapasowych istnieją tylko na serwerze Acronis Backup & Recovery 10 Management Server.

Aby sprawdzić, czy dane są skutecznie chronione, nie trzeba łączyć się z każdym komputerem z osobna. Zamiast tego należy sprawdzić skumulowany status zasad (s. 330) na wszystkich komputerach zarządzanych, na których zastosowano te zasady.

Aby dowiedzieć się, czy zasady tworzenia kopii zapasowych są obecnie wdrażane, odwoływane czy aktualizowane, należy sprawdzić stan wdrażania (s. 330) zasad.

Sposób pracy z widokiem zasad tworzenia kopii zapasowych

- Przyciski funkcjonalne **paska narzędzi** służą do tworzenia nowych zasad, stosowania istniejących zasad do komputerów lub wykonywania innych operacji związanych z zasadami tworzenia kopii zapasowych (s. 332).
- Karty panelu **Informacja** służą do wyświetlania szczegółowych informacji o wybranych zasadach oraz do wykonywania dodatkowych operacji, takich jak odwoływanie zasad, wyświetlanie szczegółów komputera (grupy), na którym zastosowano zasady, itp. Panel jest domyślnie zwinięty. Aby rozwinąć panel, należy kliknąć przycisk.  Zawartość panelu jest także zduplikowana w oknie Policy details (s. 334) (Szczegóły zasad).
- Funkcje filtrowania i sortowania (s. 333) tabeli zasad umożliwiają łatwe przeglądanie i sprawdzanie.

Stany wdrażania zasad tworzenia kopii zapasowych

Stan wdrażania zasad tworzenia kopii zapasowych to kombinacja stanów wdrażania na wszystkich komputerach, na których zastosowano zasady. Jeśli na przykład zasady zastosowano na trzech komputerach i na pierwszym komputerze mają one stan „Wdrażanie”, na drugim stan „Aktualizacja”, a na trzecim stan „Wdrożone”, stan zasad będzie miał wartość „Wdrażanie, Aktualizacja, Wdrożone”.

Stan wdrażania zasad tworzenia kopii zapasowych w grupie komputerów to kombinacja stanów wdrażania na komputerach należących do grupy.

Aby uzyskać szczegółowe informacje na temat stanów wdrażania zasad tworzenia kopii zapasowych, zapoznaj się z sekcją Stan i statusy zasad tworzenia kopii zapasowych (s. 78).

Statusy zasad tworzenia kopii zapasowych

Status zasad tworzenia kopii zapasowych to skumulowany status statusów zasad na wszystkich komputerach, na których zastosowano zasady. Jeśli na przykład zasady zastosowano na trzech komputerach i na pierwszym komputerze mają one status „OK”, na drugim status „Ostrzeżenie”, a na trzecim status „Błąd”, status zasad będzie miał wartość „Błąd”.

Status zasad tworzenia kopii zapasowych w grupie komputerów to skumulowany status statusów zasad na komputerach należących do grupy.

Poniższa tabela przedstawia podsumowanie możliwych statusów zasad tworzenia kopii zapasowych.

	Status	Sposób ustalania	Sposób obsługi
1	**Błąd**	Status zasad na co najmniej jednym komputerze ma wartość „Błąd”. W przeciwnym razie zobacz 2.	Wyświetl dziennik lub zidentyfikuj zadania zakończone niepowodzeniem, aby poznać przyczynę niepowodzenia, a następnie wykonaj co najmniej jedną z poniższych czynności: ▪ Usuń przyczynę niepowodzenia -> [opcjonalnie] Ręcznie uruchom zadanie zakończone niepowodzeniem. ▪ Przeprowadź edycję zasad tworzenia kopii zapasowych, aby

			zapobiec niepowodzeniu w przyszłości.
2	**Ostrzeżenie**	Status zasad na co najmniej jednym komputerze ma wartość „Ostrzeżenie”. W przeciwnym razie zobacz 3.	Wyświetl dziennik, aby przeczytać ostrzeżenia -> [opcjonalnie] Wykonaj odpowiednie czynności, aby zapobiec ostrzeżeniom lub niepowodzeniu w przyszłości.
3	**OK**	Status zasad na wszystkich komputerach ma wartość „OK”.	Nie jest wymagana żadna akcja. Zwróć uwagę, że jeśli zasad tworzenia kopii zapasowych nie zastosowano na żadnym komputerze, ich stan także ma wartość „OK”.

Co zrobić, jeśli zasady mają status Błąd

1. Aby poznać przyczynę niepowodzenia, wykonaj co najmniej jedną z poniższych czynności:
   - Kliknij hiperłącze **Błąd**, aby wyświetlić wpis dziennika dotyczący najnowszego błędu.
   - Wybierz zasady i kliknij **Wyświetl zadania**. Sprawdź zadania, których ostatnim wynikiem jest **Zakończone niepowodzeniem**: wybierz zadanie, a następnie kliknij **Wyświetl dziennik**. Wybierz wpis dziennika i kliknij **Wyświetl szczegóły**. Ta metoda jest wygodna, gdy stan zasad ma wartość Wdrożone, co oznacza, że zadania zasad już istnieją na komputerach zarządzanych.
   - Wybierz zasady i kliknij **Wyświetl dziennik**. Sprawdź wpisy dziennika dotyczące wartości „Błąd”, aby poznać przyczynę niepowodzenia: wybierz wpis dziennika i kliknij **Wyświetl szczegóły**. Ta metoda jest wygodna, gdy zasady zawierają błędy podczas wdrażania, odwoływania lub aktualizowania.

   *Jeśli jest zbyt dużo zadań, w widoku **Zadania** należy zastosować filtr **Ostatni wynik -> Zakończone niepowodzeniem**. Zadania zakończone niepowodzeniem można również sortować według planów tworzenia kopii zapasowych lub według komputerów.*

   *Jeśli jest zbyt dużo wpisów dziennika, w widoku **Dziennik** należy zastosować filtr Błąd. Wpisy mające wartość „Błąd” można również sortować według planów tworzenia kopii zapasowych, jednostek zarządzanych lub komputerów.*

2. Gdy przyczyna niepowodzenia jest jasna, wykonaj co najmniej jedną z poniższych czynności:
   - Usuń przyczynę niepowodzenia. Następnie może być konieczne ręczne uruchomienie zadania zakończonego niepowodzeniem w celu zachowania spójności schematu tworzenia kopii zapasowych, np. jeśli zasady są oparte na schemacie GFS lub Wieża Hanoi.
   - Przeprowadź edycję zasad tworzenia kopii zapasowych, aby zapobiec niepowodzeniu w przyszłości.

*Szybki dostęp do wpisów dziennika mających wartość „Błąd” można uzyskać za pomocą sekcji **Działania** na pulpicie nawigacyjnym.*

Co zrobić, jeśli zasady mają status Ostrzeżenie

1. Aby poznać przyczynę ostrzeżenia, wykonaj co najmniej jedną z poniższych czynności:
   - Kliknij hiperłącze **Ostrzeżenie**, aby wyświetlić wpis dziennika dotyczący najnowszego ostrzeżenia.
   - Wybierz zasady i kliknij **Wyświetl zadania**. Sprawdź zadania, których ostatnim wynikiem jest **Wykonane pomyślnie z ostrzeżeniami**: wybierz zadanie, a następnie kliknij **Wyświetl dziennik**. Ta metoda jest wygodna, gdy stan zasad ma wartość Wdrożone, co oznacza, że zadania zasad już istnieją na komputerach zarządzanych.
   - Wybierz zasady i kliknij **Wyświetl dziennik**. Sprawdź wpisy dziennika dotyczące wartości „Ostrzeżenie”, aby poznać przyczynę ostrzeżeń: wybierz wpis dziennika i kliknij **Wyświetl**

szczegóły. Ta metoda jest wygodna, gdy zasady zawierają błędy podczas wdrażania, odwoływania lub aktualizowania.

*Jeśli jest zbyt dużo zadań, w widoku **Zadania** należy zastosować filtr **Ostatni wynik -> Wykonane pomyślnie z ostrzeżeniami**. Zadania wykonane pomyślnie z ostrzeżeniem można również sortować według planów tworzenia kopii zapasowych lub według komputerów.*

*Jeśli jest zbyt dużo wpisów dziennika, w widoku **Dziennik** należy zastosować filtr Ostrzeżenie. ⚠ Wpisy mające wartość „Ostrzeżenie" można również sortować według planów tworzenia kopii zapasowych, jednostek zarządzanych lub komputerów.*

2. Kiedy przyczyna ostrzeżenia stanie się jasna, można wykonać czynności mające zapobiec pojawianiu się ostrzeżeń lub niepowodzeń w przyszłości.

*Szybki dostęp do wpisów dziennika mających wartość „Ostrzeżenie" można uzyskać za pomocą sekcji **Działania** na pulpicie nawigacyjnym.*

Co zrobić, jeśli zasady mają status OK

Nie trzeba wykonywać żadnej czynności.

Czynności dotyczące zasad tworzenia kopii zapasowych

Wszystkie opisane poniżej operacje wykonuje się poprzez kliknięcie odpowiednich elementów na **pasku narzędzi** zadań. Operacje można także wykonywać za pomocą menu kontekstowego (poprzez kliknięcie prawym przyciskiem myszy wybranej zasady tworzenia kopii zapasowych) lub przy użyciu paska **Czynności dotyczące „nazwa zasad tworzenia kopii zapasowych"** w panelu **Czynności i narzędzia**.

Poniżej przedstawiono wytyczne dotyczące wykonywania operacji na zasadach tworzenia kopii zapasowych.

Zadanie	Działanie
Utwórz zasady tworzenia kopii zapasowej	Kliknij **Utwórz zasady tworzenia kopii zapasowych**. Procedura tworzenia zasad tworzenia kopii zapasowych została opisana szczegółowo w sekcji Tworzenie zasad tworzenia kopii zapasowych (s. 395).
Zastosuj zasady do komputerów lub grup	Kliknij **Zastosuj do**. W oknie Wybór komputera (s. 333) określ komputery (grupy), do których zostaną zastosowane wybrane zasady tworzenia kopii zapasowych. Jeśli komputer jest aktualnie w trybie offline, zasady zostaną wdrożone, kiedy komputer ponownie przejdzie w tryb online.
Edytuj zasady	Kliknij **Edytuj**. Edycja zasad odbywa się w ten sam sposób co ich tworzenie (s. 395). Po dokonaniu edycji zasad serwer zarządzania aktualizuje zasady na wszystkich komputerach, na których są one wdrożone.
Usuń zasady	Kliknij **Usuń**. Spowoduje to odwołanie zasad z komputerów, na których zostały wdrożone, oraz ich usunięcie z serwera zarządzania. Jeśli komputer jest aktualnie w trybie offline, zasady zostaną odwołane, kiedy komputer ponownie przejdzie w tryb online.
Wyświetl szczegóły zasad lub odwołaj zasady	Kliknij **Wyświetl szczegóły**. W oknie Policy details (s. 334) (Szczegóły zasad) sprawdź informacje dotyczące wybranych zasad. Można także odwołać zasady z komputerów lub grup, do których

	zastosowano zasady.
Wyświetl zadania zasad	Kliknij **Wyświetl zadania**. W widoku Zadania (s. 366) zostanie wyświetlona lista zadań związanych z wybranymi zasadami.
Wyświetl dziennik zasad	Kliknij **Wyświetl dziennik**. W widoku Dziennik (s. 368) zostanie wyświetlona lista wpisów dziennika związanych z wybranymi zasadami.
Odśwież listę zadań	Kliknij **Odśwież**. Konsola zarządzania zaktualizuje listę zasad tworzenia kopii zapasowych z serwera zarządzania przy użyciu najnowszych informacji. Mimo że lista zasad jest odświeżana automatycznie w oparciu o zdarzenia, dane mogą nie zostać pobrane natychmiast z serwera zarządzania ze względu na pewne opóźnienie. Po ręcznym odświeżeniu są wyświetlane najbardziej aktualne dane.

Wybór komputerów

Aby zastosować zasady tworzenia kopii zapasowych do komputerów lub grup komputerów

1. Określ, czy wybrane zasady tworzenia kopii zapasowych mają zostać zastosowane do:
   - **Grup**

     W drzewie grup wybierz grupy, do których zostaną zastosowane zasady. W prawej części okna jest wyświetlana lista komputerów w wybranej grupie.
   - **Poszczególnych komputerów**

     W drzewie grup wybierz żądaną grupę. Następnie w prawej części okna wybierz komputery, do których zostaną zastosowane zasady tworzenia kopii zapasowych.
2. Kliknij **OK**.

Serwer Acronis Backup & Recovery 10 Management Server wdroży zasady na wybranych komputerach oraz komputerach należących do wybranych grup.

Filtrowanie i sortowanie zasad tworzenia kopii zapasowych

Poniżej przedstawiono wytyczne dotyczące filtrowania i sortowania zasad tworzenia kopii zapasowych.

Zadanie	Działanie
Sortuj zasady tworzenia kopii zapasowych według dowolnej kolumny	Kliknij nagłówek kolumny, aby posortować zasady tworzenia kopii zapasowych w porządku rosnącym. Kliknij ponownie nagłówek kolumny, aby posortować zasady tworzenia kopii zapasowych w porządku malejącym.
Filtruj zasady tworzenia kopii zapasowych według nazwy/właściciela	Wpisz nazwę zasad lub właściciela w polach pod odpowiednim nagłówkiem kolumny. Zostanie wyświetlona lista zasad tworzenia kopii zapasowych, których nazwy (lub nazwy właściciela) są całkowicie lub częściowo zgodne z wprowadzoną wartością.

Filtruj zasady tworzenia kopii zapasowych według stanu wdrażania, stanu, typu źródła, ostatniego wyniku lub harmonogramu	W polu pod odpowiednim nagłówkiem kolumny wybierz żądaną wartość z listy.

Konfigurowanie tabeli zasad tworzenia kopii zapasowych

Domyślnie w tabeli jest wyświetlanych siedem kolumn, a pozostałe są ukryte. Sposób przedstawiania kolumn można dostosować do swoich potrzeb i preferencji.

Aby wyświetlić lub ukryć kolumny

1. Kliknij prawym przyciskiem myszy nagłówek kolumny, aby wyświetlić menu kontekstowe. Zaznaczone elementy menu odpowiadają nagłówkom kolumn wyświetlanych w tabeli.
2. Kliknij elementy, które chcesz wyświetlić/ukryć.

Policy details (Szczegóły zasad)

Na pięciu kartach okna **Policy details** (Szczegóły zasad) są zgromadzone wszystkie informacje dotyczące wybranych zasad tworzenia kopii zapasowych. Okno umożliwia wykonywanie operacji na komputerach i grupach komputerów, do których zastosowane są te zasady.

Te informacje są także zduplikowane na panelu **Informacje**.

Zasady tworzenia kopii zapasowych

Na tej karcie są wyświetlane informacje o wybranych zasadach.

Źródło

Na tej karcie są wyświetlane informacje o typie źródła, którego kopia zapasowa jest wykonywana, a także o regułach wyboru źródła.

Miejsce docelowe

Na tej karcie są wyświetlane informacje o miejscu docelowym kopii zapasowych.

Ustawienia

Na tej karcie są wyświetlane informacje o schemacie tworzenia kopii zapasowych używanym przez zasady, a także o opcjach tworzenia kopii zapasowych, które zostały zmodyfikowane względem ustawień domyślnych.

Zastosowane do

Na tej karcie jest wyświetlana lista komputerów i grup, do których zastosowane są wybrane zasady.

Czynności

Zadanie	Działanie
Wyświetl szczegóły komputera (grupy)	Kliknij **Wyświetl szczegóły**. W oknie Machine details (s. 342) (Szczegóły komputera)/Group details (s. 351) (Szczegóły grupy) sprawdź wszystkie informacje dotyczące wybranego komputera (lub wybranej grupy).
Wyświetl zadania komputera (grupy)	Kliknij **Wyświetl zadania**. W widoku Zadania (s. 366) zostanie wyświetlona lista zadań przefiltrowana według wybranego komputera (grupy).

Wyświetl dziennik komputera (grupy)	Kliknij **Wyświetl dziennik**. W widoku Dziennik (s. 368) zostanie wyświetlona lista wpisów dziennika przefiltrowana według wybranego komputera (grupy).
Odwołaj zasady z komputera (grupy)	Kliknij **Odwołaj**. Serwer zarządzania odwoła zasady z wybranego komputera lub grupy komputerów. Zasady pozostaną obecne na serwerze zarządzania.

7.1.3 Komputery fizyczne

Program Acronis Backup & Recovery 10 umożliwia administratorowi ochronę danych i wykonywanie operacji zarządzania na wielu komputerach. Administrator dodaje komputer do serwera zarządzania, używając nazwy lub adresu IP komputera, importuje komputery z usługi Active Directory lub z plików tekstowych. Po zarejestrowaniu (s. 427) na serwerze zarządzania komputer staje się dostępny do grupowania, stosowania zasad tworzenia kopii zapasowych i monitorowania działań związanych z ochroną danych.

W celu oszacowania, czy dane są skutecznie chronione na komputerze zarządzanym, administrator serwera zarządzania sprawdza status tego komputera. Status komputera jest definiowany jako najpoważniejszy status ze wszystkich planów tworzenia kopii zapasowych (s. 205) (zarówno lokalnych, jak i centralnych) istniejących na komputerze oraz wszystkich zasad tworzenia kopii zapasowych (s. 330) zastosowanych na komputerze. Może mieć wartość „OK”, „Ostrzeżenia” lub „Błędy”.

Grupy

Administrator serwera zarządzania może łączyć komputery w grupy. Komputer może być członkiem więcej niż jednej grupy. Wewnątrz każdej grupy utworzonej przez administratora można utworzyć jedną lub więcej grup zagnieżdżonych.

Łączenie w grupy umożliwia organizowanie ochrony danych według działów firmy, domen Active Directory lub jednostek administracyjnych w ramach domeny, różnych populacji użytkowników, lokalizacji miejsc itp.

Głównym celem łączenia w grupy jest ochrona wielu komputerów według tych samych zasad. Kiedy komputer znajduje się w grupie, są do niego stosowane zasady grupy, a nowe zadania są tworzone na podstawie tych zasad. Po usunięciu komputera z grupy zasady stosowane do grupy zostają wycofane z komputera wraz z zadaniami utworzonymi na podstawie tych zasad.

Grupa wbudowana — grupa zawsze istniejąca na serwerze zarządzania. Nie można jej usunąć ani zmienić jej nazwy. Grupa wbudowana nie może zawierać grup zagnieżdżonych. Do grupy wbudowanej można stosować zasady tworzenia kopii zapasowych. Przykładem grupy wbudowanej jest grupa **Wszystkie komputery fizyczne**, która obejmuje wszystkie komputery zarejestrowane na serwerze zarządzania.

Grupy niestandardowe — grupy tworzone ręcznie przez administratora serwera zarządzania.

- *Grupy statyczne*

  Grupy statyczne obejmują komputery ręcznie dodane do grupy przez administratora. Członek statyczny pozostaje w grupie do czasu jego wycofania z grupy lub usunięcia odpowiedniego komputera zarządzanego z serwera zarządzania przez administratora.
- *Grupy dynamiczne*

Grupy dynamiczne obejmują komputery dodawane automatycznie na podstawie kryteriów określanych przez administratora. Po określeniu kryteriów serwer zarządzania rozpoczyna badanie właściwości istniejących komputerów oraz analizuje każdy nowo zarejestrowany komputer. Komputer, który spełnia dane kryterium dynamiczne, pojawi się we wszystkich grupach stosujących to kryterium.

Aby dowiedzieć się więcej na temat łączenia komputerów w grupy, zapoznaj się z sekcją Łączenie zarejestrowanych komputerów w grupy (s. 70).

Aby dowiedzieć się więcej na temat stosowania zasad do komputerów i grup, zapoznaj się z sekcją Zasady komputerów i grup (s. 73).

Sposób pracy z komputerami

- Najpierw dodaj komputery do serwera zarządzania. Komputery można dodawać po wybraniu widoku **Komputery fizyczne** lub grupy **Wszystkie komputery fizyczne** w drzewie **Nawigacja**.
- Wybierz grupę, w której znajduje się wymagany komputer, a następnie wybierz komputer.
- Przyciski funkcjonalne **paska narzędzi** służą do wykonywania działań na komputerze (s. 339).
- Karty panelu **Informacja** służą do wyświetlania szczegółowych informacji o wybranym komputerze i wykonywania dodatkowych operacji, takich jak uruchamianie/zatrzymywanie zadań, odwoływanie zasad, badanie dziedziczenia zasad itp. Panel jest domyślnie zwinięty. Aby rozwinąć panel, należy kliknąć przycisk. Zawartość panelu jest także zduplikowana w oknie **Machine details** (s. 342) (Szczegóły komputera).
- Funkcje filtrowania i sortowania (s. 347) umożliwiają łatwe przeglądanie i sprawdzanie wybranych komputerów.

Sposób pracy z grupami

- W widoku **Komputery fizyczne** wybierz grupę.
- Przyciski funkcjonalne paska narzędzi służą do wykonywania działań w wybranej grupie (s. 348).
- Karty panelu **Informacja** służą do wyświetlania szczegółowych informacji o wybranej grupie i wykonywania dodatkowych operacji, takich jak odwoływanie zasad lub badanie dziedziczenia zasad. Panel jest domyślnie zwinięty. Aby rozwinąć panel, należy kliknąć przycisk. Zawartość panelu jest także zduplikowana w oknie **Group details** (s. 351) (Szczegóły grupy).

Czynności dotyczące komputerów

Rejestrowanie komputerów na serwerze zarządzania

Po dodaniu lub zaimportowaniu komputera do grupy **Wszystkie komputery fizyczne** zostanie on zarejestrowany na serwerze zarządzania. Na zarejestrowanych komputerach można wdrożyć zasady tworzenia kopii zapasowych i wykonać inne operacje zarządzania scentralizowanego. Rejestracja polega na ustanowieniu relacji zaufania między agentem znajdującym się na komputerze a serwerem zarządzania.

Po wybraniu widoku **Komputery fizyczne** lub grupy **Wszystkie komputery fizyczne** w drzewie Nawigacja dostępne staną się czynności dodawania i importowania.

Zadanie	Czynności
Dodawanie nowego komputera do serwera zarządzania	Kliknij **Dodaj komputer do AMS**. W oknie **Dodaj komputer** (s. 339) wybierz komputer, który ma być dodany do serwera zarządzania.

Importowanie komputerów z usługi Active Directory	Kliknij **Importuj komputery z usługi Active Directory**. W oknie **Importuj komputery z usługi Active Directory** (s. 339) określ komputery lub jednostki organizacyjne z komputerami, które chcesz zaimportować na serwer zarządzania.
Importowanie komputerów z pliku tekstowego	Kliknij **Importuj komputery z pliku**. W oknie **Importuj komputery z pliku** (s. 341) wskaż plik .txt lub .csv z nazwami (lub adresami IP) komputerów, które mają być zaimportowane na serwer zarządzania.

Konsola zarządzania kontaktuje się z agentem i rozpoczyna procedurę rejestracji. Ponieważ rejestracja wymaga udziału agenta, nie jest możliwa, gdy komputer jest w trybie offline.

Dodatkowy agent, który jest zainstalowany na zarejestrowanym komputerze, automatycznie staje się zarejestrowany na tym samym serwerze zarządzania. Istnieje możliwość jednoczesnego rejestrowania i wyrejestrowywania wielu agentów.

Stosowanie zasad

Zadanie	Czynności
Stosowanie zasad tworzenia kopii zapasowych do komputera	Kliknij **Zastosuj zasady tworzenia kopii zapasowej**. W oknie **Wybór zasad** określ zasady tworzenia kopii zapasowych, które chcesz zastosować do wybranego komputera.

Czynności grupowania

Zadanie	Czynności
Utworzenie niestandardowej grupy statycznej lub dynamicznej	Kliknij **Utwórz grupę**. W oknie **Utwórz grupę** (s. 349) określ wymagane parametry grupy. Nowa grupa zostanie utworzona w grupie, do której należy wybrany komputer (nie dotyczy wbudowanej grupy **Wszystkie komputery fizyczne**).
Dodawanie komputera do innej grupy statycznej	Kliknij **Dodaj do innej grupy**. W oknie **Dodaj do grupy** (s. 341) określ grupę, do której ma zostać skopiowany wybrany komputer. Zasady tworzenia kopii zapasowych stosowane do grup, do których należy komputer, zostaną zastosowane także do komputera.
Dla komputerów w grupach niestandardowych	
Dodawanie komputerów do grupy statycznej	Kliknij **Dodaj komputery do grupy**. W oknie **Dodaj komputery do grupy** (s. 342) wybierz komputery, które chcesz dodać.
Przenoszenie komputera do innej grupy statycznej.	Kliknij **Przenieś do innej grupy**. W oknie **Przenieś do grupy** (s. 342) wybierz grupę, do której komputer ma być przeniesiony. Wszystkie zasady tworzenia kopii zapasowych stosowane do grupy, do której należał komputer, zostaną wycofane. Zasady tworzenia kopii zapasowych stosowane do grupy, do której teraz należy komputer, zostaną także zastosowane do komputera.
Usuwanie komputera z bieżącej grupy statycznej	Kliknij **Usuń z grupy**.

	Zasady tworzenia kopii zapasowych stosowane do grupy zostaną automatycznie wycofane z komputera.

Usuwanie wybranego komputera z serwera zarządzania

Zadanie	Czynności
Usunięcie komputera z serwera zarządzania	Kliknij **Usuń komputer z AMS**. W rezultacie zasady tworzenia kopii zapasowych zostaną wycofane, a skróty do skarbców centralnych zostaną usunięte z komputera. Jeśli komputer nie jest aktualnie dostępny, czynności te zostaną wykonane na komputerze zaraz po tym, gdy stanie się on dostępny dla serwera zarządzania.

Inne czynności

Operacje zarządzania bezpośredniego	
Tworzenie planu tworzenia kopii zapasowych na komputerze	Kliknij **Kopia zapasowa**. Operację tę opisano szczegółowo w sekcji Tworzenie planu tworzenia kopii zapasowych (s. 219).
Odzyskiwanie danych	Kliknij **Odzyskaj**. Operację tę opisano szczegółowo w sekcji Odzyskiwanie danych.
Bezpośrednie połączenie z komputerem	Kliknij **Połącz bezpośrednio.** Pozwala nawiązać bezpośrednie połączenie z komputerem zarządzanym. Umożliwia administrowanie komputerem zarządzanym i wykonanie wszystkich operacji zarządzania bezpośredniego.
Inne operacje	
Wyświetlenie szczegółowych informacji o komputerze	Kliknij **Wyświetl szczegóły**. W oknie **Szczegóły komputera** (s. 342) zapoznaj się z informacjami o danym komputerze.
Wyświetlenie zadań istniejących na komputerze	Kliknij **Wyświetl zadania**. W widoku **Zadania** (s. 366) zostanie wyświetlona lista zadań istniejących na komputerze.
Wyświetlenie wpisów dziennika komputera	Kliknij **Wyświetl dziennik**. W widoku **Dziennik** (s. 368) zostanie przedstawiona lista wpisów dziennika komputera.
Aktualizacja wszystkich informacji związanych z komputerem	Kliknij **Synchronizuj**. Serwer zarządzania uzyska z komputera najbardziej aktualne informacje o nim i wprowadzi je do bazy danych. Poza synchronizacją automatycznie odświeżona zostanie lista komputerów.
Odświeżenie listy komputerów	Kliknij **Odśwież**. Konsola zarządzania zaktualizuje listę komputerów o najnowsze informacje z serwera zarządzania. Mimo że lista komputerów jest odświeżana automatycznie na podstawie zdarzeń, ze względu na pewne opóźnienie dane z serwera zarządzania mogą nie pojawić się natychmiast. Po ręcznym odświeżeniu wyświetlane są najbardziej aktualne dane.

Dodawanie komputera do serwera zarządzania

Aby umożliwić wdrażanie zasad tworzenia kopii zapasowych z serwera zarządzania Acronis Backup & Recovery 10 Management Server na zarządzanym komputerze i wykonywanie innych operacji zarządzania scentralizowanego, należy zarejestrować komputer na serwerze zarządzania.

Aby dodać komputer

1. W drzewie **Nawigacja** wybierz **Komputery fizyczne**.
2. Kliknij **Dodaj komputer do AMS** na pasku narzędzi.
3. W polu **Adres IP/nazwa** wprowadź nazwę komputera lub jego adres IP albo kliknij **Przeglądaj** i wyszukaj komputer w sieci.

   Uwaga dla użytkowników wersji Virtual Edition: *W przypadku dodawania hosta VMware ESX/ESXi wprowadź adres IP urządzenia wirtualnego, na którym jest uruchomiony komponent Acronis Backup & Recovery 10 Agent dla ESX/ESXi.*

4. Określ nazwę i hasło użytkownika należącego do grupy **Administratorzy** na komputerze.

   Uwaga dla użytkowników wersji Virtual Edition: *W przypadku dodawania hosta VMware ESX/ESXi określ nazwę i hasło użytkownika centrum vCenter lub hosta ESX/ESXi.*

   Kliknij **Opcje** i określ następujące elementy:

   - **Nazwa użytkownika**. Wprowadzając nazwę konta użytkownika usługi Active Directory, należy określić również nazwę domeny (DOMENA\Nazwa_użytkownika).
   - **Hasło**. Hasło konta.

   Zaznacz pole wyboru **Zapisz hasło**, aby zapamiętać hasło dla kolejnych połączeń.
5. Kliknij **OK**.

Inicjowanie rejestracji po stronie komputera

Procedurę rejestracji można zainicjować po stronie komputera.

1. Podłącz konsolę do komputera, na którym jest zainstalowany agent Acronis Backup & Recovery 10. W przypadku wyświetlenia pytania o poświadczenia określ poświadczenia członka grupy **Administratorzy** na komputerze.
2. Z menu wybierz **Opcje** > **Opcje komputera** > **Zarządzanie komputerem**.
3. Wybierz **Zarządzanie scentralizowane** i określ serwer zarządzania, na którym chcesz zarejestrować komputer. Aby uzyskać szczegółowe informacje, zobacz „Zarządzanie komputerem (s. 105)”.

Importowanie komputerów z usługi Active Directory

Aby zaimportować komputery z usługi Active Directory

1. W drzewie **Nawigacja** wybierz **Komputery fizyczne** lub **Wszystkie komputery fizyczne**.
2. Kliknij **Importuj komputery z usługi Active Directory** na pasku narzędzi.
3. W polu **Wyszukaj** wpisz nazwę komputera (lub jednostki organizacyjnej), a następnie kliknij **Szukaj**. Można użyć gwiazdki (*), aby zastąpić zero lub więcej znaków w nazwie komputera (lub jednostki organizacyjnej).

   W lewej części okna są wyświetlane nazwy komputerów (lub jednostek organizacyjnych), które są całkowicie lub częściowo zgodne z wprowadzoną wartością. Kliknij element, który chcesz dodać w celu zaimportowania, a następnie kliknij **Dodaj>>**. Element zostanie przeniesiony do prawej części okna. Aby dodać wszystkie znalezione elementy, kliknij **Dodaj wszystko>>**.

Jeśli znaleziono ponad 1000 pasujących elementów, zostanie wyświetlony tylko pierwszy tysiąc. W takim przypadku zaleca się zawężenie wyszukiwania i ponowienie operacji.

W prawej części okna są wyświetlane elementy wybrane do zaimportowania. W razie potrzeby usuń blednie wybrane elementy, używając odpowiednich przycisków **Usuń** i **Usuń wszystko**.

4. Kliknij **OK**, aby rozpocząć importowanie.

Synchronizowanie komputerów z plikiem tekstowym

W czasie synchronizacji serwer zarządzania dopasowuje grupę **Wszystkie komputery fizyczne** do listy komputerów umieszczonej w pliku .txt lub .csv. Serwer zarządzania:

- Dodaje komputery, które znajdują się na liście, ale nie są zarejestrowane.
- Usuwa zarejestrowane komputery, który nie znajdują się na liście.
- Usuwa i próbuje ponownie dodać zarejestrowane komputery, które znajdują się na liście, ale ich bieżąca dostępność (s. 342) jest określona jako **Wycofany**.

Oznacza to, że w grupie **Wszystkie komputery fizyczne** będą się znajdować tylko te komputery, które są umieszczone w pliku.

Wymagania dotyczące pliku tekstowego

Plik powinien zawierać po jednej nazwie lub jednym adresie IP komputera w każdym wierszu.

Przykład:

```
Nazwa_komputera_1
Nazwa_komputera_2
192.168.1.14
192.168.1.15
```

Określenie pustego pliku powoduje usunięcie wszystkich komputerów fizycznych z serwera zarządzania.

Zarejestrowany komputer musi być określony za pomocą swojego adresu rejestracji. Oznacza to, że należy podać dokładnie tę samą nazwę hosta, w pełni kwalifikowaną nazwę domeny (FQDN) lub adres IP, które określono podczas początkowego dodawania komputera do serwera zarządzania. W przeciwnym razie komputer zostanie usunięty i dodany jako nowy. Oznacza to, że z komputera zostaną odwołane wszystkie zasady — odziedziczone i zastosowane bezpośrednio — oraz utraci on członkostwo w grupach statycznych.

Adres rejestracji każdego komputera znajduje się w kolumnie **Adres rejestracji** w dowolnym widoku serwera zarządzania obejmującym dany komputer (kolumna ta jest domyślnie ukryta).

Aby uniknąć rozbieżności, można na początku zaimportować komputery z pliku tekstowego. Plik ten można później odpowiednio modyfikować przez dodawanie lub usuwanie komputerów. Nie należy jednak zmieniać nazw ani adresów tych komputerów, które mają pozostać zarejestrowane.

Aby zsynchronizować komputery z plikiem tekstowym

1. W drzewie **Nawigacja** wybierz **Komputery fizyczne** lub **Wszystkie komputery fizyczne**.
2. Kliknij **Synchronizuj komputery z plikiem tekstowym** na pasku narzędzi.
3. W polu **Ścieżka** wprowadź ścieżkę do pliku .txt lub .csv zawierającego listę komputerów lub kliknij **Przeglądaj** i wybierz plik w oknie **Przeglądaj**.
4. W opcji **Ustawienia logowania** określ nazwę i hasło użytkownika należącego do grupy Administratorzy na wszystkich komputerach umieszczonych w pliku.

5. Kliknij **OK**, aby rozpocząć synchronizację komputerów.

Narzędzie wiersza polecenia do synchronizacji

Serwer zarządzania Acronis Backup & Recovery 10 Management Server udostępnia narzędzie wiersza polecenia, które umożliwia utworzenie pliku wsadowego i zaplanowanie zadania synchronizacji przy użyciu harmonogramu systemu Windows.

Aby zsynchronizować komputery za pomocą pliku tekstowego przy użyciu wiersza polecenia

1. Zaloguj się jako członek grupy zabezpieczeń **Acronis Centralized Admins**.
2. W wierszu polecenia zmień katalog na folder, w którym został zainstalowany serwer zarządzania Acronis Backup & Recovery 10 Management Server. Domyślnie jest to folder **C:\Program Files\Acronis\AMS**.
3. Uruchom następujące polecenie:

   ```
   syncmachines [ścieżka_do_pliku] {nazwa_użytkownika hasło}
   ```

   gdzie:

   - [ścieżka_do_pliku] to ścieżka do pliku .txt lub .csv zawierającego listę komputerów. Narzędzie nie obsługuje spacji w nazwie ścieżki.
   - {nazwa_użytkownika hasło} należą do użytkownika, który jest członkiem grupy administratorów na wszystkich komputerach znajdujących się na liście w pliku. Jeśli nie określono inaczej, na wszystkich komputerach będzie używany mechanizm rejestracji jednokrotnej.

Importowanie komputerów z pliku tekstowego

Aby zaimportować komputery z pliku

1. W drzewie **Nawigacja** wybierz **Komputery fizyczne** lub **Wszystkie komputery fizyczne**.
2. Na pasku narzędzi kliknij **Importuj komputery z pliku**.
3. W polu **Ścieżka** wprowadź ścieżkę do pliku .txt lub .csv albo kliknij **Przeglądaj** i w oknie **Przeglądaj** wybierz plik.

   Plik .txt lub .csv powinien zawierać nazwy komputerów lub ich adresy IP. W każdym wierszu powinien znajdować się jeden komputer.

   Przykład:

   ```
   Nazwa_komputera_1
   Nazwa_komputera_2
   192.168.1.14
   192.168.1.15
   ```

4. W opcji **Ustawienia logowania** określ nazwę i hasło użytkownika należącego do grupy Administratorzy na wszystkich komputerach umieszczonych w pliku.
5. Aby rozpocząć importowanie, kliknij **OK**.

Dodawanie komputera do innej grupy

Aby dodać wybrany komputer do innej grupy

1. Wybierz grupę, do której ma zostać dodany komputer.
2. Kliknij **OK**.

Dodawany komputer stanie się członkiem jednej lub większej liczby grup. W wyniku tego zasady tworzenia kopii zapasowych, które zastosowano do pierwszej grupy, pozostaną aktywne na komputerze, a zasady tworzenia kopii zapasowych, które zastosowano do drugiej i kolejnych grup, zostaną wdrożone na tym komputerze.

Przenoszenie komputera do innej grupy

Aby przenieść wybrany komputer do innej grupy

1. W drzewie grup wybierz grupę, do której zostanie przeniesiony komputer.
2. Kliknij **OK**.

Przenoszony komputer opuści grupę i stanie się członkiem innej grupy. W wyniku tego zasady tworzenia kopii zapasowych, które zastosowano do pierwszej grupy, zostaną odwołane z komputera, a zasady tworzenia kopii zapasowych, które zastosowano do drugiej grupy, zostaną wdrożone na tym komputerze.

Dodawanie komputerów do grupy

Aby dodać komputery do wybranej grupy

1. W drzewie grup wybierz grupę, której komputery chcesz dodać.
2. W prawej części okna wybierz komputery.
3. Aby dodać więcej komputerów z innych grup, powtórz kroki 1 i 2 dla każdej grupy.
4. Kliknij **OK**, aby dodać komputery.

Kiedy komputery pojawią się w grupie, zostaną na nich wdrożone zasady zastosowane do grupy (jeśli istnieją). Jeśli jakieś wybrane komputery nie będą dostępne lub osiągalne w danym momencie, czynność zostanie zachowana na serwerze zarządzania jako oczekująca i zostanie wykonana natychmiast, kiedy komputer stanie się dostępny dla serwera.

Szczegóły komputera

Zebrane na czterech kartach wszystkie informacje o wybranym komputerze. Pozwala administratorowi serwera zarządzania na wykonanie operacji związanych z istniejącymi na komputerze planami i zadaniami tworzenia kopii zapasowych oraz z zasadami stosowanymi na komputerze.

Informacje te są także dostępne na panelu **Informacje**.

Komputer

Na tej karcie wyświetlane są następujące informacje o zarejestrowanym komputerze:

- **Nazwa** — nazwa wybranego komputera (pobrana z pola **Nazwa komputera** w systemie Windows).
- **Adres IP** — adres IP wybranego komputera.
- **Stan** — status komputera. Określony jako najpoważniejszy status (s. 206) wszystkich planów tworzenia kopii zapasowych (lokalnych i scentralizowanych) istniejących na komputerze oraz zasad tworzenia kopii zapasowych (s. 330) zastosowanych do komputera.
- **Ostatnie połączenie** — czas, który upłynął od ostatniego połączenia serwera zarządzania z komputerem.
- **Ostatnia pomyślnie utworzona kopia zapasowa** — czas, który upłynął od ostatniego pomyślnego utworzenia kopii zapasowej.
- **Dostępność:**
  - **Online** — komputer jest dostępny dla serwera zarządzania. Oznacza to, że ostatnie połączenie serwera zarządzania z komputerem zostało nawiązane pomyślnie. Próby połączeń są wykonywane co dwie minuty.

- **Offline** — komputer nie jest dostępny dla serwera zarządzania: został wyłączony lub odłączono od niego kabel sieciowy.
- **Nieznany** — ten status jest wyświetlany po dodaniu komputera lub uruchomieniu usługi serwera zarządzania, a przed pierwszym połączeniem serwera z komputerem.
- **Wycofany** — komputer został zarejestrowany na innym serwerze zarządzania lub w ustawieniu **Opcje > Opcje komputera > Zarządzanie komputerem** (s. 105) został wybrany parametr **Zarządzanie autonomiczne**. Oznacza to, że nie jest możliwe sterowanie komputerem z bieżącego serwera zarządzania. Aby odzyskać możliwość sterowania komputerem, należy określić adres serwera zarządzania w ustawieniach **Zarządzanie komputerem**.
- **Wygasł** — upłynął okres próbny agenta komputera. Aby określić pełny klucz licencyjny, użyj funkcji **Zmień licencję** lub uruchom program instalacyjny i postępuj zgodnie z jego instrukcjami.

- **Zainstalowane agenty** — pełne nazwy zainstalowanych na komputerze agentów programu Acronis.
- **System operacyjny** — system operacyjny uruchomiony w agencie komputera.
- **Procesor** — typ procesora w zarządzanym komputerze.
- **Zegar procesora** — szybkość taktowania procesora.
- **Pamięć RAM** — rozmiar pamięci.
- **Komentarze** — opis komputera (pobrany z pola **Opis komputera** w systemie Windows).

Zasady tworzenia kopii zapasowych

Wyświetla listę zasad tworzenia kopii zapasowych stosowanych do wybranego komputera i umożliwia administratorowi serwera zarządzania wykonywanie następujących operacji:

Zadanie	Działanie
Wyświetl szczegóły zasad	Kliknij **Wyświetl szczegóły**. W oknie **Policy details** (s. 334) (Szczegóły zasad) sprawdź wszystkie informacje dotyczące wybranych zasad tworzenia kopii zapasowych.
Wyświetl zadania zasad	Kliknij **Wyświetl zadania**. W widoku **Zadania** (s. 366) zostanie wyświetlona lista zadań związanych z wybranymi zasadami.
Wyświetl dziennik zasad	Kliknij **Wyświetl dziennik**. W widoku **Dziennik** (s. 368) zostanie wyświetlona lista wpisów dziennika związanych z wybranymi zasadami tworzenia kopii zapasowych.
Odwołaj zasady z komputera.	Kliknij **Odwołaj**. Serwer zarządzania odwoła zasady z komputera. Zasady pozostają na serwerze zarządzania. Jeżeli komputer jest członkiem grupy, do której stosowane są zasady, można je odwołać z komputera bez uprzedniego wycofania komputera z grupy.
Sprawdź pochodzenie stosowanych zasad	Kliknij **Eksploruj dziedziczenie**. W oknie **Kolejność dziedziczenia** (s. 347) zostanie wyświetlona kolejność dziedziczenia zasad stosowanych do komputera.

Filtrowanie i sortowanie

Filtrowanie i sortowanie zasad tworzenia kopii zapasowych następuje w taki sam sposób jak w widoku **Zasady tworzenia kopii zapasowych**. Aby uzyskać szczegółowe informacje, zapoznaj się z sekcją Filtrowanie i sortowanie zasad tworzenia kopii bezpieczeństwa (s. 333).

Plany i zadania

Pokazuje listę planów (lokalnych i centralnych) oraz zadań istniejących na wybranym komputerze.

Operacje

Poniżej przedstawiono wytyczne dotyczące Poniżej przedstawiono wytyczne dotyczące wykonywania operacji na planach i zadaniach tworzenia kopii zapasowych.

Zadanie	Działanie
Wyświetl szczegóły planu lub zadania	**Plan tworzenia kopii zapasowej** Kliknij **Wyświetl szczegóły**. W oknie **Szczegóły planu** (s. 215) przejrzyj informacje szczegółowe dotyczące planu. **Zadanie** Kliknij **Wyświetl szczegóły**. W oknie **Szczegóły zadania** (s. 213) przejrzyj informacje szczegółowe dotyczące zadania.
Wyświetl dziennik planu lub zadania	**Plan tworzenia kopii zapasowej** Kliknij **Wyświetl dziennik**. Nastąpi przeniesienie do widoku **Dziennik** (s. 216), zawierającego listę wpisów do dziennika dotyczących planu. **Zadanie** Kliknij **Wyświetl dziennik**. Nastąpi przeniesienie do widoku **Dziennik** (s. 216), zawierającego listę wpisów do dziennika dotyczących zadania.
Uruchom plan lub zadanie	**Plan tworzenia kopii zapasowej** Kliknij **Uruchom**. W oknie **Uruchom plan tworzenia kopii zapasowej** (s. 213) wybierz zadanie do uruchomienia. Uruchomienie planu tworzenia kopii zapasowej spowoduje natychmiastowe rozpoczęcie wybranego zadania, niezależnie od jego harmonogramu i warunków. **Zadanie** Kliknij **Uruchom**. Zadanie zostanie wykonane natychmiast, niezależnie od harmonogramu i warunków.

Zatrzymaj plan lub zadanie	**Plan tworzenia kopii zapasowej** Kliknij **Zatrzymaj**. Zatrzymanie wykonywanego planu tworzenia kopii zapasowej spowoduje zatrzymanie wszystkich jego zadań. W związku z tym wszystkie operacje zadania zostaną przerwane. **Zadanie** Kliknij **Zatrzymaj**. *Co się stanie, kiedy zatrzymam zadanie?* Ogólnie rzecz biorąc, zatrzymanie zadania powoduje przerwanie jego operacji (tworzenie kopii zapasowej, odzyskiwanie, sprawdzanie poprawności, eksportowanie, konwersja, migracja). Zadanie przejdzie najpierw do stanu Zatrzymywane, a następnie do stanu Bezczynne. Harmonogram zadania, jeśli został utworzony, pozostanie ważny. Aby zakończyć operację, trzeba będzie ponownie uruchomić zadania. ▪ Zadanie odzyskiwania (z kopii zapasowej dysku): docelowy wolumin zostanie usunięty, a jego miejsce stanie się nieprzydzielone, tak samo jak w przypadku niepowodzenia odzyskiwania. Aby odzyskać „utracony" wolumin, należy ponownie uruchomić zadanie. ▪ Zadanie odzyskiwania (z kopii zapasowej plików): przerwana operacja może spowodować zmiany w folderze docelowym. W zależności od tego, w jakim momencie zadanie zostało zatrzymane, niektóre pliki mogą zostać odzyskane, a inne nie. Aby odzyskać wszystkie pliki, należy ponownie uruchomić zadanie.
Edytuj plan lub zadanie	**Plan tworzenia kopii zapasowej** Kliknij **Edytuj**. Edycja planu tworzenia kopii zapasowej odbywa się w ten sam sposób co jego tworzenie (s. 219), z wyjątkiem następujących **ograniczeń**: Jeżeli utworzone archiwum nie jest puste (to znaczy zawiera kopie zapasowe), zmiana właściwości schematu tworzenia kopii zapasowych nie zawsze jest możliwa. 1. Nie można zmienić schematu na Dziadek-ojciec-syn lub Wieża Hanoi. 2. Jeżeli stosowany jest schemat Wieża Hanoi, zmiana liczby poziomów jest niemożliwa. We wszystkich innych przypadkach schemat można zmienić i powinien on nadal działać tak, jakby istniejące archiwa zostały utworzone na podstawie nowego schematu. W przypadku archiwów pustych wszystkie zmiany są możliwe. *Dlaczego nie mogę edytować planu tworzenia kopii zapasowych?* ▪ Plan tworzenia kopii zapasowych jest obecnie uruchomiony. Edycja uruchomionego planu tworzenia kopii zapasowych jest niemożliwa. ▪ Plan tworzenia kopii zapasowych ma pochodzenie centralne. Bezpośrednia edycja scentralizowanych planów tworzenia kopii zapasowych jest niemożliwa. Trzeba edytować oryginalne zasady tworzenia kopii zapasowych. **Zadanie** Kliknij **Edytuj**. *Dlaczego nie mogę edytować zadania?* ▪ Zadanie należy do planu tworzenia kopii zapasowych. Bezpośrednia edycja jest możliwa tylko w przypadku zadań, które nie należą do planu tworzenia kopii zapasowych, takich jak zadanie odzyskiwania. Jeśli trzeba zmodyfikować zadanie należące do lokalnego planu tworzenia kopii zapasowych, należy dokonać edycji

	planu tworzenia kopii zapasowych. Zadanie należące do scentralizowanego planu tworzenia kopii zapasowych można zmodyfikować poprzez edycję zasad scentralizowanych, które obejmują plan.
Usuń plan lub zadanie	**Plan tworzenia kopii zapasowej** Kliknij **Usuń**. *Co się zdarzy, jeżeli usunę plan tworzenia kopii zapasowych?* Usunięcie planu spowoduje usunięcie wszystkich jego zadań. *Dlaczego nie mogę usunąć planu tworzenia kopii zapasowych?* ▪ Plan tworzenia kopii zapasowych jest w stanie uruchomienia. Nie można usunąć planu tworzenia kopii zapasowych, jeżeli przynajmniej jedno z jego zadań jest uruchomione. ▪ Plan tworzenia kopii zapasowych ma pochodzenie centralne. Administrator serwera zarządzania może usunąć plan scentralizowany poprzez wycofanie zasad tworzenia kopii zapasowych, które składają się na plan. **Zadanie** Kliknij **Usuń**. *Dlaczego nie mogę usunąć zadania?* ▪ Zadanie należy do planu tworzenia kopii zapasowych. Zadania należącego do planu tworzenia kopii zapasowych nie można usunąć w oddzieleniu od planu. Edytuj plan, aby usunąć zadanie lub cały plan.
Odśwież tabelę	Kliknij **Odśwież**. Konsola zarządzania zaktualizuje listę zadań istniejących na komputerach przy użyciu najnowszych informacji. Mimo że lista jest odświeżana automatycznie w oparciu o zdarzenia, dane mogą nie zostać pobrane natychmiast z komputera zarządzanego ze względu na pewne opóźnienie. Po ręcznym odświeżeniu są wyświetlane najbardziej aktualne dane.

Filtrowanie i sortowanie

Filtrowanie i sortowanie zasad tworzenia kopii zapasowych następuje w taki sam sposób jak w widoku **Zasady tworzenia kopii zapasowych** w celu bezpośredniego zarządzania. Aby uzyskać szczegółowe informacje, zapoznaj się z sekcją Filtrowanie i sortowanie planów tworzenia kopii bezpieczeństwa i zadań (s. 212).

Członek grupy

Karta pojawia się tylko po dodaniu wybranego komputera do jednej lub więcej grup niestandardowych i wyświetla listę grup, których członkiem jest komputer.

Operacje

Zadanie	Działanie
Wyświetl szczegóły grupy	Kliknij **Wyświetl szczegóły**. Nastąpi przeniesienie do okna Szczegóły grupy, gdzie można sprawdzić wszystkie informacje dotyczące grupy.
Wyświetl zadania dotyczące grupy	Kliknij **Wyświetl zadania**. Nastąpi przeniesienie do widoku Zadania ze wstępnie przefiltrowanymi zadaniami

	dotyczącymi wybranej grupy kopii zapasowej.
Wyświetl dziennik dotyczący grupy	Kliknij **Wyświetl dziennik**. Zostanie otwarty widok Dziennika ze wstępnie przefiltrowanymi wpisami dziennika wybranej grupy.
Usuń komputer z grupy	Kliknij **Usuń**. Plany scentralizowane wdrożone w grupie nadrzędnej nie będą już miały wpływu na ten komputer.

Obsługiwane maszyny wirtualne

Na tej karcie wyświetlana jest lista maszyn obsługiwanych na wybranym serwerze wirtualizacji lub zarządzanych przez określone urządzenie wirtualne.

Na podstawie listy obsługiwanych maszyn wirtualnych można utworzyć grupę dynamiczną. W tym celu kliknij **Utwórz grupę dynamiczną**. Utworzona grupa będzie dostępna w widoku Maszyny wirtualne (s. 354).

Kolejność dziedziczenia

Okno **Kolejność dziedziczenia** umożliwia sprawdzenie pochodzenia zasad stosowanych do komputera.

Zasada bezpośrednio zastosowana do komputera jest wyświetlana w następujący sposób:
Nazwa komputera

Zasada zastosowana do komputera poprzez dziedziczenie jest wyświetlana jak w przykładzie poniżej:
Grupa1 > **Grupa2** > Grupa3 > Komputer1

Grupa1 w katalogu głównym obejmuje grupę *Grupa2*, do której zasady są stosowane bezpośrednio. *Grupa2* z kolei obejmuje grupę podrzędną *Grupa3*, która dziedziczy zasady od nadrzędnej i stosuje je odpowiednio do komputera *Komputer1*.

Komputer (lub grupa), do którego zostały zastosowane zasady bezpośrednio, jest wyróżniony pogrubioną czcionką i oznaczony ikoną.

Wszystkie elementy są interaktywne, to znaczy po kliknięciu komputera lub grupy, otwiera się grupa nadrzędna.

Filtrowanie i sortowanie komputerów

Zadanie	Działanie
Sortuj komputery według dowolnej kolumny	Kliknij nagłówek kolumny, aby posortować komputery w porządku rosnącym. Kliknij ponownie nagłówek kolumny, aby posortować komputery w porządku malejącym.
Filtruj komputery według nazwy	Wpisz nazwę komputera w polu pod odpowiednim nagłówkiem kolumny. Zostanie wyświetlona lista komputerów, których nazwy są całkowicie lub częściowo zgodne z wprowadzoną wartością.

Filtruj komputery według stanu, ostatniego połączenia, ostatniej kopii zapasowej lub dostępności	W polu pod odpowiednim nagłówkiem kolumny wybierz żądaną wartość z listy.

Konfigurowanie tabeli komputerów

Domyślnie w tabeli jest wyświetlanych pięć kolumn, a pozostałe są ukryte. W razie potrzeby można ukryć wyświetlane kolumny i wyświetlić ukryte kolumny.

Aby wyświetlić lub ukryć kolumny

1. Kliknij prawym przyciskiem myszy nagłówek kolumny, aby wyświetlić menu kontekstowe. Zaznaczone elementy menu odpowiadają nagłówkom kolumn wyświetlanych w tabeli.
2. Kliknij elementy, które chcesz wyświetlić/ukryć.

Czynności dotyczące grup

Czynności są dostępne po wybraniu widoku  **Komputery fizyczne** w drzewie **Nawigacja** i kliknięciu grupy.

Poniżej przedstawiono wytyczne dotyczące wykonywania czynności na wybranych grupach.

Zadanie	Działanie
Utwórz niestandardową grupę statyczną lub dynamiczną	Kliknij  **Utwórz grupę**. W oknie **Utwórz grupę** (s. 349) określ wymagane parametry grupy. Grupy niestandardowe można utworzyć w folderze głównym ( **Komputery fizyczne**) lub w innych grupach niestandardowych.
Zastosuj zasady tworzenia kopii zapasowych do grupy	Kliknij  **Zastosuj zasady tworzenia kopii zapasowej**. W oknie **Wybór zasad** określ zasady tworzenia kopii zapasowych, które chcesz zastosować do wybranej grupy. Jeśli w wybranej grupie istnieją grupy podrzędne, zasady tworzenia kopii zapasowych zostaną zastosowane również do tych grup podrzędnych.
Wyświetl szczegółowe informacje o grupie	Kliknij  **Wyświetl szczegóły**. W oknie **Group details** (s. 351) (Szczegóły grupy) sprawdź informacje dotyczące wybranej grupy.
Zmień nazwę grupy niestandardowej lub podrzędnej	Kliknij  **Zmień nazwę**. W kolumnie **Nazwa** wpisz nową nazwę wybranej grupy. Nie można zmienić nazw grup wbudowanych.
Edytuj grupę niestandardową	Kliknij  **Edytuj**. W oknie **Edytuj grupę** (s. 351) zmień wymagane parametry grupy.
Przenieś grupę niestandardową do innej grupy	Kliknij  **Przenieś do**. W oknie **Przenieś do grupy** (s. 351) określ grupę, która stanie się nową grupą nadrzędną wybranej grupy.
Usuń grupę niestandardową	Kliknij  **Usuń**. Usunięcie grupy nadrzędnej powoduje także usunięcie jej grup podrzędnych. Zasady tworzenia kopii zapasowych, które zostały zastosowane do grupy nadrzędnej i odziedziczone przez jej grupy podrzędne, zostaną odwołane ze wszystkich członków usuniętych grup. Z kolei zasady, które zastosowano bezpośrednio do członków, będą

	nadal obowiązywać.
Odśwież listę grup	Kliknij **Odśwież**. Konsola zarządzania zaktualizuje listę grup z serwera zarządzania przy użyciu najnowszych informacji. Mimo że lista grup jest odświeżana automatycznie w oparciu o zdarzenia, dane mogą nie zostać pobrane natychmiast z serwera zarządzania ze względu na pewne opóźnienie. Po ręcznym odświeżeniu są wyświetlane najbardziej aktualne dane.

Utworzenie niestandardowej grupy statycznej lub dynamicznej

Aby utworzyć grupę

1. W polu **Nazwa grupy** wprowadź nazwę tworzonej grupy.
2. Wybierz typ grupy:
   a. **Statyczny** — aby utworzyć grupę, do której komputery będą dodawane ręcznie.
   b. **Dynamiczny** — aby utworzyć grupę, która będzie zawierać komputery dodawane automatycznie na podstawie określonych kryteriów.

      Kliknij **Dodaj kryteria** i wybierz wzór kryterium.

      - **System operacyjny,**

        Do grupy dynamicznej będą należeć wszystkie komputery, na których jest uruchomiony wybrany system operacyjny.
      - **Jednostka organizacyjna** (s. 350)

        Do grupy dynamicznej będą należeć wszystkie komputery należące do określonej jednostki organizacyjnej (OU).
      - **Zakres adresów IP**

        Do grupy dynamicznej będą należeć wszystkie komputery o adresie IP należącym do podanego zakresu adresów.
      - **Wymieniony w pliku txt/csv** (s. 350)

        Do grupy dynamicznej będą należeć wszystkie komputery znajdujące się w określonym pliku .txt lub .csv.
3. W polu **Komentarze** wprowadź opis tworzonej grupy.
4. Kliknij **OK**.

Dodawanie wielu kryteriów

Dodanie wielu kryteriów pozwala utworzyć warunek zgodnie z następującymi zasadami:

a) Wszystkie wyrażenia tego samego kryterium są łączone dodawaniem logicznym (LUB)

Na przykład następujący zestaw kryteriów:

System operacyjny: Windows Server 2008

System operacyjny: Windows Server 2003

spowoduje dodanie do grupy wszystkich komputerów, na których jest uruchomiony system Windows 2000 LUB Windows 2003.

b) Różne kryteria są łączone iloczynem logicznym (I)

Na przykład następujący zestaw kryteriów:

System operacyjny: Windows Server 2008

System operacyjny: Windows Server 2003

Jednostka organizacyjna: SERWERY

Zakres adresów IP: 192.168.17.0–192.168.17.55

spowoduje dodanie do tej samej grupy wszystkich komputerów z systemem operacyjnym Windows 2000 lub Windows 2003, należących do jednostki organizacyjnej SERWERY i o adresach IP z zakresu 192.168.17.0–192.168.17.55.

Jak długo członek grupy dynamicznej należy do grupy?

Członek grupy dynamicznej pozostaje w niej tak długo, jak spełnia kryteria. Usunięcie członka z grupy następuje automatycznie, jeśli:

- wprowadzone zmiany spowodują, że członek przestanie spełniać kryteria lub
- administrator zmieni kryteria tak, że przestaną być spełniane przez członka.

Jedynym sposobem ręcznego usunięcia komputera z grupy dynamicznej jest usunięcie go z serwera zarządzania.

Kryterium jednostki organizacyjnej

Kryterium jednostki organizacyjnej jest określone dla domeny, w której aktualnie znajduje się serwer zarządzania. Kryterium wygląda w następujący sposób: *OU=OU1*

Wybierz jednostkę organizacyjną z drzewa Active Directory, klikając **Przeglądaj**, lub wprowadź ją ręcznie. Jeśli w opcjach serwera zarządzania nie zostały określone poświadczenia dostępu do domeny, program poprosi o ich wprowadzenie. Poświadczenia zostaną zapisane w opcji Poświadczenia umożliwiające uzyskanie dostępu do domeny (s. 103).

Przypuśćmy, że domena *us.corp.przyklad.com* ma jednostkę organizacyjną OU1 (która jest na poziomie głównym), OU1 ma OU2, a OU2 ma OU3. Chcesz dodać komputery z jednostki OU3. Kryterium będzie wyglądać w następujący sposób: *OU=OU3, OU=OU2, OU=OU1*

Jeśli jednostka OU3 zawiera kontenery podrzędne i chcesz dodać komputery z tych kontenerów do grupy, zaznacz pole wyboru **Uwzględnij kontenery podrzędne**.

Kryterium Wymieniony w pliku txt/csv

Jeśli użyjesz tego kryterium, grupa dynamiczna obejmie komputery z listy podanej w określonym pliku .txt lub .csv.

W przypadku późniejszej modyfikacji tego pliku zawartość grupy ulegnie odpowiedniej zmianie. Plik jest sprawdzany co 15 minut.

Późniejsze usunięcie tego pliku lub jego niedostępność spowoduje, że zawartość grupy będzie odpowiadać liście ostatnio przechowywanej w pliku.

Wymagania dotyczące pliku tekstowego

Plik powinien zawierać po jednej nazwie lub jednym adresie IP komputera w każdym wierszu.

Przykład:

```
Nazwa_komputera_1
Nazwa_komputera_2
192.168.1.14
192.168.1.15
```

Zarejestrowany komputer musi być określony za pomocą swojego adresu rejestracji. Oznacza to, że należy podać dokładnie tę samą nazwę hosta, w pełni kwalifikowaną nazwę domeny (FQDN) lub adres IP, które określono podczas początkowego dodawania komputera do serwera zarządzania.

W przeciwnym przypadku komputer nie zostanie dodany do grupy. Adres rejestracji każdego komputera znajduje się w kolumnie **Adres rejestracji** w dowolnym widoku serwera zarządzania obejmującym dany komputer (kolumna ta jest domyślnie ukryta).

Przenoszenie grupy do innej grupy

Aby przenieść wybraną grupę do innej grupy lub folderu głównego

1. W drzewie grup kliknij grupę, do której chcesz przenieść wybraną grupę. Można przenieść grupę niestandardową dowolnego typu (statyczną lub dynamiczną) do innej grupy niestandardowej dowolnego typu lub do folderu głównego.

   Folder główny drzewa komputerów zawiera *grupy pierwszego poziomu*. Grupy zawierające inne grupy są nazywane *grupami nadrzędnymi*. Grupy znajdujące się w grupach nadrzędnych są nazywane *grupami podrzędnymi*. Wszystkie zasady tworzenia kopii zapasowych zastosowane do grupy nadrzędnej zostaną zastosowane również do jej grup podrzędnych.
2. Kliknij **OK**.

Edytowanie grup niestandardowych

Edycja grupy niestandardowej odbywa się w ten sam sposób co jej tworzenie (s. 349).

Zmiana typu grupy spowoduje jej konwersję. Dowolną niestandardową grupę statyczną można przekonwertować na grupę dynamiczną lub odwrotnie.

- Podczas konwersji grupy statycznej na dynamiczną należy określić kryteria grupowania. Z grupy dynamicznej zostaną usunięci wszyscy członkowie istniejący w grupie statycznej, którzy nie spełniają określonych kryteriów.
- Podczas konwersji grupy dynamicznej na statyczną dostępne są dwie opcje: można pozostawić bieżącą zawartość grupy lub opróżnić grupę.

Szczegóły grupy

Na dwóch kartach zgromadzone są wszystkie informacje dotyczące wybranej grupy. Okno umożliwia wykonywanie operacji na zasadach zastosowanych do grupy.

Te informacje są także zduplikowane na panelu **Informacje**.

Grupa

Na tej karcie są wyświetlane następujące informacje dotyczące grupy:

- **Nazwa** — nazwa wybranej grupy;
- **Grupa nadrzędna** (tylko w przypadku podgrup) — nazwa grupy nadrzędnej;
- **Komputery** — liczba komputerów w grupie;
- **Typ** — typ grupy (statyczna lub dynamiczna);
- **Kryterium** (tylko w przypadku grup dynamicznych) — kryteria łączenia w grupy;
- **Komentarze** — opis grupy (jeżeli został określony).

Zasady tworzenia kopii zapasowych

Wyświetla listę zasad tworzenia kopii zapasowych dotyczących grupy i umożliwia wykonanie następujących operacji:

Zadanie	Działanie
Wyświetl szczegóły zasad	Kliknij **Wyświetl szczegóły**. W oknie Policy details (s. 334) (Szczegóły zasad) sprawdź wszystkie informacje dotyczące wybranych zasad tworzenia kopii zapasowych.
Wyświetl zadania zasad	Kliknij **Wyświetl zadania**. W widoku Zadania (s. 366) zostanie wyświetlona lista zadań związanych z wybranymi zasadami.
Wyświetl dziennik zasad	Kliknij **Wyświetl dziennik**. W widoku Dziennik (s. 368) zostanie wyświetlona lista wpisów dziennika związanych z wybranymi zasadami tworzenia kopii zapasowych.
Odwołaj zasady z grupy	Kliknij **Odwołaj**. Serwer zarządzania odwołuje zasady z grupy. Podczas przesyłania zmian do komputerów i usuwania przez agentów planów tworzenia kopii zapasowych, stan zasad grupy to **Odwoływanie**. Zasady pozostają na serwerze zarządzania.
Sprawdź pochodzenie zasad stosowanych do grupy	Kliknij **Eksploruj reguły dziedziczenia**. W oknie **Kolejność dziedziczenia** (s. 352) zostanie wyświetlona kolejność dziedziczenia zasad stosowanych do grupy.

Filtrowanie i sortowanie

Filtrowanie i sortowanie zasad tworzenia kopii zapasowych następuje w taki sam sposób jak w widoku Zasady tworzenia kopii zapasowych. Aby uzyskać szczegółowe informacje, zobacz sekcję Filtrowanie i sortowanie zasad tworzenia kopii zapasowych (s. 333).

Kolejność dziedziczenia

W oknie **Kolejność dziedziczenia** można sprawdzić pochodzenie zasad stosowanych do grupy.

Zasady bezpośrednio stosowane do grupy są wyświetlane w następujący sposób:
Nazwa grupy

Poniższy przykład ilustruje sposób, w jaki są wyświetlane zasady stosowane do grupy poprzez dziedziczenie.
Grupa1 > **Grupa2** > Grupa3

Grupa1 w katalogu głównym obejmuje grupę *Grupa2*, do której zasady są stosowane bezpośrednio. *Grupa2* z kolei obejmuje grupę podrzędną *Grupa3*, która dziedziczy zasady od nadrzędnej.

Grupa, do której zostały zastosowane zasady bezpośrednio jest wyróżniona pogrubioną czcionką i oznaczona ikoną.

Wszystkie elementy są interaktywne, to znaczy po kliknięciu grupy, otwiera się grupa nadrzędna.

7.1.4 Maszyny wirtualne

Maszynami wirtualnymi można zarządzać centralnie przy użyciu następujących metod (stosowanych oddzielnie lub łącznie):

Dodawanie maszyny wirtualnej jako komputera fizycznego

Zainstaluj na maszynie wirtualnej komponent Acronis Backup & Recovery 10 Agent for Windows lub Agent for Linux i zarejestruj (s. 339) ją na serwerze zarządzania. Maszyna będzie traktowana jak komputer fizyczny. Pojawi się ona w obszarze **Komputery z agentami**, w grupie **Wszystkie komputery z agentami**.

Ta metoda jest wygodna, gdy:

- maszyna nie znajduje się na serwerze wirtualizacji;
- nie posiadasz licencji wersji Acronis Backup & Recovery 10 Virtual Edition;
- wersja Virtual Edition nie obsługuje tworzenia kopii zapasowych na poziomie hiperwizora dla tego konkretnego programu wirtualizującego;
- musisz pokonać ograniczenia kopii zapasowej na poziomie hiperwizora.

Dodawanie maszyny wirtualnej jako maszyny wirtualnej

Na serwerze zarządzania Acronis Backup & Recovery 10 Management Server komputer jest traktowany jako maszyna wirtualna, jeśli można wykonać jego kopię zapasową z hosta wirtualizacji, nie instalując na nim agenta. Umożliwia to wersja Acronis Backup & Recovery 10 Advanced Server Virtual.

Maszynę wirtualną do serwera zarządzania można dodać na kilka sposobów:

- Włącz integrację (s. 104) serwera zarządzania z serwerem vCenter Server.

  Rezultat. Maszyny wirtualne zarządzane przez serwer vCenter Server znajdują się w obszarze **Maszyny wirtualne** w grupie **Wszystkie maszyny wirtualne**. Maszyny wyglądają na niezarządzane (są wyszarzone), ale można tworzyć ich kopie zapasowe, jeśli podczas integracji włączono automatyczne wdrażanie agentów.
- Zainstaluj i skonfiguruj komponent Agent for ESX(i) VMware vSphere (Virtual Appliance) lub Agent for ESX(i) VMware vSphere (Windows). Zarejestruj agenta na serwerze zarządzania.

  Rezultat. Komputer z agentem (urządzenie wirtualne lub host systemu Windows) pojawi się w obszarze **Komputery z agentami** w grupie **Wszystkie komputery z agentami**. Maszyny wirtualne zarządzane przez agenta znajdują się w obszarze **Maszyny wirtualne** w grupie **Wszystkie maszyny wirtualne**.
- Zainstaluj komponent Agent for Hyper-V na hoście Hyper-V lub na wszystkich węzłach klastra Hyper-V. Zarejestruj agenty na serwerze zarządzania.

  Rezultat. Host (węzły) Hyper-V pojawi się w obszarze **Komputery z agentami** w grupie **Wszystkie komputery z agentami**. Maszyny wirtualne zarządzane przez agentów znajdują się w obszarze **Maszyny wirtualne** w grupie **Wszystkie maszyny wirtualne**.

Maszyny wirtualne dodane do serwera zarządzania jako maszyny wirtualne są widoczne w grupie **Maszyny wirtualne** w drzewie **Nawigacja**. W tej sekcji omówiono dostępne operacje na tych maszynach.

Maszyny wirtualne na serwerze zarządzania

Dostępność maszyn wirtualnych

Maszyny wirtualne są wyświetlane jako dostępne, gdy agent jest dostępny dla serwera zarządzania, a maszyny są dostępne dla agenta. Lista maszyn wirtualnych jest odświeżana dynamicznie przy każdej synchronizacji serwera zarządzania z agentami.

Gdy serwer wirtualizacji lub urządzenie wirtualne staje się niedostępne lub zostaje wycofane, maszyny wirtualne zostają wyszarzone.

Gdy maszyny wirtualne stają się niedostępne dla agenta (np. po usunięciu maszyn z magazynu serwera wirtualizacji, usunięciu ich z dysku lub wyłączeniu albo awarii lub odłączeniu magazynu serwera), maszyny te znikają z grup **Wszystkie maszyny wirtualne** oraz z innych grup, w których się znajdowały. Zadania tworzenia kopii zapasowych tych maszyn wirtualnych kończą się niepowodzeniem, a w dzienniku jest umieszczany odpowiedni wpis. W rezultacie zasady generujące będą miały status błędu.

Stan online lub offline maszyny wirtualnej nie wpływa na jej kopie zapasowe — można je wykonywać w obu stanach.

Zasady dotyczące maszyn wirtualnych

Każdą zasadę tworzenia kopii zapasowych dysków i woluminów można zastosować zarówno do maszyn wirtualnych, jak i fizycznych komputerów. Zasad tworzenia kopii zapasowych na poziomie plików nie można stosować do maszyn wirtualnych. Aby uzyskać więcej informacji o tworzeniu kopii zapasowych i odzyskiwaniu maszyn wirtualnych, obsługiwanych systemów operacyjnych-gości i konfiguracji dysków, zobacz Tworzenie kopii zapasowych maszyn wirtualnych (s. 54).

Co dzieje się po zastosowaniu zasad do grupy maszyn wirtualnych?

Kopia zapasowa każdej maszyny zostanie utworzona w ramach osobnego zadania i umieszczona w osobnym archiwum. W domyślnej nazwie archiwum zostanie uwzględniona nazwa maszyny wirtualnej oraz nazwa zasad. Zalecamy zachowanie domyślnych nazw archiwów. Pozwoli to łatwo odnaleźć w skarbcu kopie zapasowe każdej maszyny.

Grupowanie maszyn wirtualnych

Sekcja **Maszyny wirtualne** drzewa nawigacyjnego zawiera jedną wbudowaną grupę o nazwie **Wszystkie maszyny wirtualne**. Nie można ręcznie zmodyfikować tej grupy, usunąć jej ani przenieść. Można wobec niej zastosować zasady tworzenia kopii zapasowych dysków lub woluminów.

Można utworzyć zarówno statyczne, jak i dynamiczne grupy maszyn wirtualnych. Do grupy statycznej można dodać każdą aktualnie dostępną maszynę wirtualną. Nie można tworzyć grup łączących komputery fizyczne i maszyny wirtualne.

Dynamiczne kryteria przynależności do grupy dla maszyn wirtualnych obejmują:

- **Typ serwera wirtualizacji (Hyper-V, ESX/ESXi).**

Za pomocą tego kryterium można utworzyć dynamiczną grupę maszyn wirtualnych obsługiwanych na wszystkich zarejestrowanych serwerach Hyper-V (lub, odpowiednio, ESX/ESXi). Każda maszyna dodana do serwerów pojawi się w tej grupie. Każda maszyna usunięta z serwerów zniknie z tej grupy.

- **Host/urządzenie wirtualne**

Za pomocą tego kryterium można utworzyć dynamiczną grupę maszyn wirtualnych obsługiwanych na określonym serwerze wirtualizacji lub zarządzanych przez określone urządzenie wirtualne.

Integracja VMware vCenter

Jeśli używasz systemu VMware vSphere, zaleca się zintegrowanie serwera zarządzania z serwerem vCenter Server.

Aby zintegrować serwer zarządzania z serwerem VMware vCenter Server:

1. W drzewie **Nawigacja** kliknij prawym przyciskiem myszy **Maszyny wirtualne** i wybierz **Integracja VMware vCenter**.
2. Kliknij **Skonfiguruj integrację**.
3. Zaznacz pole wyboru **Włącz integrację VMware vCenter**.
4. Określ adres IP lub nazwę serwera vCenter Server i podaj odpowiednie poświadczenia dostępu.
5. Kliknij **OK**.

W rezultacie na serwerze zarządzania w sekcji **Maszyny wirtualne** zostanie wyświetlona grupa o tej samej nazwie co serwer vCenter Server. Aby uzyskać więcej informacji, zobacz „Integracja VMware vCenter (s. 104)”.

Aby usunąć integrację z serwerem VMware vCenter Server:

1. W drzewie **Nawigacja** kliknij prawym przyciskiem myszy **Maszyny wirtualne** i wybierz **Integracja VMware vCenter**.
2. Kliknij **Skonfiguruj integrację**.
3. Wyczyść pole wyboru **Włącz integrację VMware vCenter**.
4. Kliknij **OK.**

Grupa o takiej samej nazwie co serwer vCenter Server zostanie usunięta. Zasady zastosowane do tej grupy oraz do jej grup podrzędnych zostaną odwołane.

Jeśli host maszyn wirtualnych jest zarządzany przez agenta dla ESX/ESXi, maszyny pozostaną w grupie **Wszystkie maszyny wirtualne** oraz w innych grupach. Zasady zastosowane do tych grup lub bezpośrednio do maszyn będą dalej na nich działać. Oznacza to, że usuniecie integracji powoduje usunięcie tylko maszyn niemożliwych do zarządzania.

Wdrażanie i aktualizowanie Agenta dla ESX/ESXi

Serwer zarządzania Acronis Backup & Recovery 10 Management Server umożliwia łatwe wdrożenie agenta dla ESX/ESXi na każdym serwerze VMware ESX lub ESXi zawierającym maszyny wirtualne, których kopie zapasowe chcesz tworzyć.

Na każdym określonym serwerze ESX/ESXi zostanie utworzone urządzenie wirtualne z agentem, a następnie urządzenie to zostanie zarejestrowane na serwerze zarządzania. Na serwerze zarządzania pojawią się maszyny wirtualne pogrupowane dynamicznie według hostów. Umożliwi to stosowanie do maszyn zasad tworzenia kopii zapasowych oraz tworzenie kopii zapasowych poszczególnych maszyn.

Aktualizacja już zainstalowanych agentów jest przeprowadzana tak samo jak ich wdrożenie. Po wybraniu hosta lub klastra, na którym jest zainstalowany agent, zostanie wyświetlony monit o aktualizację agenta na tym hoście.

Jeśli używasz systemu VMware vSphere, przed rozpoczęciem wdrażania agenta zaleca się zintegrowanie (s. 355) serwera zarządzania z serwerem vCenter Server. Nie będzie wówczas trzeba ręcznie określać każdego hosta.

Aby wdrożyć agenta dla ESX/ESXi na serwerach VMware ESX/ESXi:

1. W drzewie **Nawigacja** kliknij prawym przyciskiem myszy **Maszyny wirtualne** lub grupę o tej samej nazwie co serwer vCenter Server.
2. Kliknij **Wdróż agenta ESX**.
3. **Hosty ESX/ESXi**

   W przypadku serwera vCenter Server zostanie wyświetlona lista hostów i klastrów ESX/ESXi uzyskanych z tego serwera. Wybierz hosty i klastry, na których chcesz wdrożyć agenta, lub zaznacz pole wyboru **Wybierz wszystko**.

   W klastrze vCenter jeden Agent dla ESX/ESXi tworzy kopie zapasowe maszyn wirtualnych znajdujących się na wszystkich hostach w klastrze. Aby uzyskać więcej informacji, zobacz „Obsługa klastrów vCenter (s. 357)”.

   Aby do listy dodać jeden host, określ jego adres IP lub nazwę. Podaj nazwę użytkownika i hasło dla każdego hosta dodawanego do listy. W tym oknie nie można określić serwera vCenter Server.

   Po wybraniu hosta lub klastra, na którym jest już zainstalowany agent, w prawym panelu okna **Wdrażanie Agenta ESX** zostanie wyświetlona opcja: **Aktualizuj agenta ESX na tym hoście**. Inne ustawienia są niedostępne. Jeśli jest konieczna tylko aktualizacja, przejdź od razu do kroku 6.
4. [Opcjonalne] **Ustawienia agenta**

   Agenty dla ESX/ESXi można wdrożyć z ustawieniami domyślnymi, ale można również określić ustawienia niestandardowe dla każdego agenta. Dostępne są następujące ustawienia:

   Magazyn danych — magazyn danych na hoście ESX/ESXi, w którym będzie przechowywane urządzenie wirtualne. W przypadku wdrażania agenta w klastrze vCenter jest to magazyn danych współużytkowany przez wszystkie serwery wchodzące w skład klastra. Aby uzyskać więcej informacji, zobacz „Obsługa klastrów vCenter (s. 357)”.

   Interfejs sieciowy — sieć wewnętrzna hosta, w której zostanie umieszczone urządzenie wirtualne. Jeśli na hoście jest dostępnych wiele sieci, program wybierze sieć najbardziej odpowiednią do pracy agenta i określi ją jako sieć **domyślną**. Można wybierać tylko te sieci, które mają połączenie z konsolą usług hosta (lub siecią zarządzania w rozumieniu terminologii systemu VMware Infrastructure). Jest to aspekt kluczowy dla poprawnej pracy agenta.

   Następne ustawienie różni się w zależności od sposobu wdrażania agenta.

   Wdrażanie za pośrednictwem serwera vCenter — **konto, które będzie używane do połączeń agenta z serwerem vCenter**.

   Wdrażanie bezpośrednio na serwerze ESX/ESXi — **konto, które będzie używane do połączeń agenta z serwerem ESX**.

   Serwer zarządzania użyje tego konta do ustanowienia zaufanej relacji z agentem podczas rejestracji. Na tym koncie będą domyślnie uruchamiane scentralizowane plany tworzenia kopii zapasowych i zadania odzyskiwania pochodzące z serwera zarządzania. Oznacza to, że konto musi mieć niezbędne uprawnienia (s. 359) na serwerze vCenter Server.

   Domyślnie oprogramowanie używa konta, które zostało już określone przez użytkownika podczas konfigurowania integracji z centrum vCenter bądź podczas uzyskiwania dostępu do serwera ESX/ESXi. W razie potrzeby można określić poświadczenia innego konta.

   Strefa czasowa urządzenia wirtualnego zostanie automatycznie dopasowana do strefy czasowej na serwerze zarządzania. Strefę czasową można zmienić bezpośrednio w graficznym interfejsie urządzenia wirtualnego zgodnie z opisem podanym w sekcji „Instalowanie komponentu ESX/ESXi Virtual Appliance”. Można też zmienić konto lub ustawienia sieciowe, jednak jeśli nie jest to absolutnie konieczne, nie zaleca się wykonywania tych czynności.
5. **Licencje**

   Kliknij **Podaj licencję**.

W przypadku instalowania wersji próbnej programu wybierz **Użyj następującego próbnego klucza licencyjnego** i wprowadź próbny klucz licencyjny. W wersji próbnej deduplikacja jest zawsze włączona.

Podczas instalowania zakupionego programu wybierz **Użyj licencji z następującego serwera Acronis License Server** i określ serwer licencji, na którym znajduje się odpowiednia liczba licencji programu Acronis Backup & Recovery 10 Advanced Server Virtual Edition. Każdy wybrany host wymaga jednej licencji.

Aby była możliwa deduplikacja kopii zapasowych, agent potrzebuje sprzedawanej oddzielnie licencji na deduplikację. Jeśli takie licencje zostały zaimportowane na serwer licencji, możesz zaznaczyć pole wyboru **Włącz deduplikację**, aby umożliwić agentom pobranie tych licencji.

Jeśli instalujesz produkt *tylko* do tworzenia kopii zapasowych online, wybierz opcję **Tylko kopia zapasowa online (klucz licencyjny nie jest wymagany)**. W przypadku tej opcji zakłada się, że posiadasz lub wykupisz subskrypcję usługi Acronis Backup & Recovery 10 Online przed wykonaniem pierwszej kopii zapasowej.

6. Kliknij **Wdróż agenta ESX**.

Monitorowanie postępów i wyników wdrażania

Tworzenie lub aktualizowanie urządzeń wirtualnych może trochę potrwać. Informacje o postępie operacji są wyświetlane u dołu widoków maszyn wirtualnych pod paskiem **Informacje**. Po utworzeniu i zarejestrowaniu urządzenia wirtualnego na serwerze zarządzania pojawi się odpowiednia grupa maszyn wirtualnych.

Jeśli wdrożenie zostało ukończone, ale brakuje grupy maszyn wirtualnych

Otwórz konsolę urządzenia wirtualnego za pomocą klienta vSphere/VMware Infrastructure i sprawdź konfigurację agenta. W razie potrzeby skonfiguruj agenta ręcznie zgodnie z opisem w sekcji „Instalowanie komponentu ESX/ESXi Virtual Appliance”. Dodaj ręcznie urządzenie wirtualne do serwera zarządzania zgodnie z opisem w sekcji „Dodawanie komputera do serwera zarządzania (s. 339)”.

Obsługa klastrów vCenter

W klastrze vCenter jeden agent dla ESX/ESXi tworzy kopie zapasowe maszyn wirtualnych obsługiwanych na wszystkich hostach klastra.

Wdrażanie agenta dla ESX/ESXi w klastrze

Konfigurując wdrażanie agenta z serwera zarządzania, można wybrać klaster jako zwykły host ESX. Urządzenie wirtualne agenta zostanie wdrożone w magazynie współużytkowanym przez wszystkie hosty klastra. Zwykle jest to udział NFS lub dysk typu SAN-LUN podłączony do każdego z hostów.

Załóżmy, że klaster składa się z trzech serwerów.

- Serwer 1 korzysta z magazynów A, B, C, D.
- Serwer 2 korzysta z magazynów C, D, E.
- Serwer 3 korzysta z magazynów B, C, D.

Urządzenie wirtualne można wdrożyć w magazynie C lub D. Jeśli żaden magazyn nie jest współużytkowany przez wszystkie serwery, można ręcznie zaimportować urządzenie wirtualne na dowolne hosty. Ta metoda zadziała, ale wydajność tworzenia kopii zapasowych będzie daleka od optymalnej.

Po wdrożeniu urządzenie wirtualne agenta może się pojawić na dowolnym z hostów zawartych w klastrze, w zależności od konfiguracji równoważenia obciążenia.

Przenoszenie urządzenia wirtualnego agenta w obrębie klastra

Jeśli usługa harmonogramu zasobów rozproszonych (Distributed Resource Scheduler — DRS) przeniesie urządzenie wirtualne na inny host, nie wpłynie to na działanie agenta.

Tworzenie klastra serwerów z już zainstalowanymi agentami

Zalecane jest usunięcie agentów dla ESX/ESXi ze wszystkich serwerów poza jednym. Zachowaj agenta, którego urządzenie wirtualne znajduje się we współużytkowanym magazynie. Ponownie uruchom urządzenie wirtualne, aby wykryło obecność klastra.

Obsługa migracji maszyn wirtualnych

W tej sekcji zostały przedstawione informacje na temat możliwości migracji maszyn wirtualnych w centrum danych przy użyciu opcji migracji serwera vCenter Server. Uwagi dotyczące wydajności dotyczą zarówno migracji „gorącej”, jak i „zimnej”.

VMotion

Narzędzie VMotion umożliwia przeniesienie stanu i konfiguracji maszyny wirtualnej na inny host, podczas gdy dyski maszyny pozostają w tej samej lokalizacji w magazynie współużytkowanym. Narzędzie VMotion jest w pełni obsługiwane, zarówno dla Agenta urządzenia ESX/ESXi Virtual Appliance, jak i maszyn wirtualnych, których kopie zapasowe są tworzone przez agenta. Podczas tworzenia kopii zapasowych może nastąpić migracja urządzenia wirtualnego lub maszyny.

Storage VMotion

Narzędzie Storage VMotion umożliwia przeniesienie dysków maszyny wirtualnej z jednego magazynu danych do innego. Migracja Agenta urządzenia ESX/ESXi Virtual Appliance przy użyciu narzędzia Storage VMotion nie jest możliwa jedynie podczas tworzenia kopii zapasowej lub odzyskiwania. Podczas migracji agent wstrzymuje wszelkie operacje tworzenia kopii zapasowych, które mają się rozpocząć. Tworzenie kopii zapasowych rozpoczyna się po zakończeniu migracji.

Migracja maszyny wirtualnej przy użyciu narzędzia Storage VMotion podczas tworzenia kopii zapasowej jest możliwa, ale utworzenie kopii może zakończyć się niepowodzeniem lub powodzeniem z ostrzeżeniami. Agent nie będzie mógł usunąć migawki utworzonej przed migracją, ponieważ maszyna nie będzie już istniała. Aby uniknąć takiej sytuacji, nie migruj maszyny wirtualnej przed zakończeniem tworzenia kopii zapasowej.

Uwagi dotyczące wydajności

Warto pamiętać, że wydajność tworzenia kopii zapasowych spada, gdy Agent dla ESX/ESXi nie ma bezpośredniego dostępu do magazynu, w którym znajdują się dyski uwzględniane w kopii zapasowej. W takim przypadku agent nie może podłączyć dysków. Uzyskuje wówczas dostęp do tych dysków przy użyciu sieci LAN. Ten proces jest dużo wolniejszy niż uzyskiwanie danych bezpośrednio z podłączonych dysków.

Dlatego dobrą praktyką jest umieszczenie Agenta urządzenia ESX/ESXi Virtual Appliance na hoście mającym dostęp do wszystkich współużytkowanych magazynów w klastrze. W takim przypadku wydajność tworzenia kopii zapasowych jest optymalna podczas każdej migracji maszyn lub urządzeń wirtualnych (w obrębie współużytkowanych magazynów). Po migracji maszyny do lokalnego magazynu na innym hoście operacje tworzenia jej kopii zapasowych będą działały wolniej.

Uprawnienia do tworzenia kopii zapasowych i odzyskiwania maszyn wirtualnych

Po wdrożeniu agenta dla ESX/ESXi na hoście lub w klastrze vCenter każdy użytkownik serwera vCenter Server może połączyć się z agentem za pomocą konsoli zarządzania. Zakres dostępnych operacji zależy od uprawnień użytkownika serwera vCenter Server. Dostępne są tylko te operacje, do których użytkownik ma uprawnienia. W tabeli poniżej podano uprawnienia wymagane do tworzenia kopii zapasowych maszyn wirtualnych ESX i ich odzyskiwania, a także do wdrażania urządzeń wirtualnych.

Jeśli agent został wdrożony bezpośrednio na hoście ESX/ESXi lub ręcznie zaimportowany na host, a chcesz umożliwić użytkownikom vCenter łączenie się z agentem oraz uwzględnić poniższe uprawnienia, połącz agenta z serwerem vCenter Server, a nie z hostem ESX/ESXi. Aby zmienić połączenie, otwórz graficzny interfejs użytkownika urządzenia wirtualnego za pomocą klienta vSphere i w ustawieniu **ESX(i)/vCenter** określ poświadczenia dostępu serwera vCenter Server.

Uprawnienia na serwerze vCenter Server lub hoście ESX/ESXi

W tabeli poniżej podano uprawnienia użytkownika serwera vCenter Server wymagane do wykonywania operacji na wszystkich hostach i klastrach vCenter.

Aby umożliwić użytkownikowi pracę tylko na określonym hoście ESX, przypisz użytkownikowi identyczne uprawnienia na hoście. Ponadto do tworzenia kopii zapasowych maszyn wirtualnych na określonym hoście ESX wymagane jest uprawnienie **Globalne** > **Licencje**.

		Operacja				
Obiekt	**Uprawnienie**	**Tworzenie kopii zapasowej maszyny wirtualnej**	**Tworzenie kopii zapasowej dysku maszyny wirtualnej**	**Odzyskiwanie na nową maszynę wirtualną**	**Odzyskiwanie na istniejącą maszynę wirtualną**	**Wdrażanie urządzenia wirtualnego**
Magazyn danych	**Przydzielanie miejsca**			+	+	+
	Przeglądanie magazynu danych					+
	Niskopoziomowe operacje na plikach					+
Globalne	**Licencje**	+ (wymagane tylko na hoście ESX)	+ (wymagane tylko na hoście ESX)	+	+	
Sieć	**Przypisywanie sieci**			+	+	+

Zasób	**Przypisywanie maszyny wirtualnej do puli zasobów**			+	+	+
Maszyna wirtualna > Konfiguracja	**Dodawanie istniejącego dysku**	+	+	+		
	Dodawanie nowego dysku			+	+	+
	Dodawanie lub usuwanie urządzenia			+		+
	Zmiana liczby procesorów			+		
	Pamięć			+		
	Usuwanie dysku	+	+	+	+	
	Zmiana nazwy			+		
	Ustawienia				+	
Maszyna wirtualna > Interakcja	**Konfigurowanie nośnika CD**			+		
	Interakcja z konsolą					+
	Wyłączanie zasilania				+	+
	Włączanie zasilania			+	+	+
Maszyna wirtualna > Inwentaryzacja	**Tworzenie na podstawie istniejącej**			+	+	
	Tworzenie nowej			+	+	+
	Usuwanie			+	+	+
Maszyna wirtualna > Zapewnianie dostępu	**Zezwalanie na dostęp do dysku**			+	+	

Maszyna wirtualna > Stan	**Tworzenie migawki**	+	+		+	+
	Usuwanie migawki	+	+		+	+

Uprawnienia do folderu

Aby umożliwić użytkownikowi pracę w określonym folderze vCenter, przypisz mu poniższe uprawnienia do folderu.

		Operacja		
Obiekt	**Uprawnienie**	**Tworzenie kopii zapasowej maszyny wirtualnej**	**Tworzenie kopii zapasowej dysku maszyny wirtualnej**	**Odzyskiwanie na istniejącą maszynę wirtualną**
Magazyn danych	**Przydzielanie miejsca**			+
Globalne	**Licencje**	+	+	+
Sieć	**Przypisywanie sieci**			+
Zasób	**Przypisywanie maszyny wirtualnej do puli zasobów**			+
Maszyna wirtualna > Konfiguracja	**Dodawanie istniejącego dysku**	+	+	
	Dodawanie nowego dysku			+
	Usuwanie dysku	+	+	+
	Ustawienia			+
Maszyna wirtualna > Interakcja	**Wyłączanie zasilania**			+
	Włączanie zasilania			+
Maszyna wirtualna > Inwentaryzacja	**Tworzenie na podstawie istniejącej**			+
	Tworzenie nowej			+
	Usuwanie			+

Maszyna wirtualna > Zapewnianie dostępu	**Zezwalanie na dostęp do dysku**			+
Maszyna wirtualna > Stan	**Tworzenie migawki**	+	+	+
	Usuwanie migawki	+	+	+

Usuwanie agenta dla ESX/ESXi

Aby usunąć agenta dla ESX/ESXi z serwera ESX/ESXi, należy usunąć odpowiednie urządzenie wirtualne. Przy włączonej integracji z centrum vCenter istnieje możliwość automatycznego usunięcia agenta dla ESX/ESXi z hostów zarządzanych przez serwer vCenter Server.

Aby automatycznie usunąć agenta dla ESX/ESXi:

1. W drzewie **Nawigacja** kliknij prawym przyciskiem myszy grupę o tej samej nazwie co serwer vCenter Server.
2. Kliknij **Usuń agenty ESX**.
3. Zostanie wyświetlona lista hostów ESX/ESXi uzyskanych z serwera vCenter Server. Wybierz hosty, z których chcesz usunąć agenty, lub zaznacz pole wyboru **Wybierz wszystko**.
4. Kliknij **Usuń agenty ESX**.

Co się stanie po usunięciu agenta

Urządzenie wirtualne zawierające agenta zostanie usunięte z dysku serwera. Maszyny wirtualne znajdujące się na danym serwerze ESX/ESXi znikną z serwera zarządzania lub staną się niedostępne dla tworzenia kopii zapasowych i odzyskiwania (jeśli integracja z centrum vCenter jest nadal włączona).

Licencja Virtual Edition na serwerze licencji nie zostanie automatycznie zwolniona. Jeśli konieczne jest zwolnienie licencji, odwołaj ją z hosta ręcznie za pomocą narzędzia **Zarządzaj licencjami**.

7.1.5 Węzły magazynowania

Węzeł magazynowania Acronis Backup & Recovery 10 ułatwia optymalne wykorzystanie różnych zasobów potrzebnych do ochrony danych przedsiębiorstw. Ten cel jest osiągany poprzez organizowanie skarbców zarządzanych (s. 428), które służą jako dedykowane magazyny archiwów kopii zapasowych przedsiębiorstwa.

Węzeł magazynowania umożliwia:

- zmniejszenie niepotrzebnego obciążenia procesorów komputerów zarządzanych dzięki zastosowaniu czyszczenia po stronie węzła magazynowania (s. 420) i sprawdzania poprawności po stronie węzła magazynowania (s. 429);
- drastyczne zmniejszenie obciążenia tworzeniem kopii zapasowych oraz ilości miejsca do przechowywania zajmowanego przez archiwa dzięki zastosowaniu deduplikacji (s. 81);
- zapobieganie dostępowi do archiwów kopii zapasowych, nawet w przypadku kradzieży nośnika magazynowego lub uzyskania dostępu do niego w wyniku przestępstwa, dzięki zastosowaniu skarbców zaszyfrowanych (s. 429).

Aby dowiedzieć się więcej o węźle Acronis Backup & Recovery 10 Storage Node, zapoznaj się z sekcją Węzeł magazynowania Acronis Backup & Recovery 10 Storage Node (s. 22).

Najważniejsze elementy widoku „Węzły magazynowania”

- **Lista węzłów magazynowania z paskiem narzędzi**

  Pasek narzędzi umożliwia wykonywanie operacji (s. 363) związanych z wybranym węzłem magazynowania. Lista zawiera węzły magazynowania w trybie online i offline dodane do serwera zarządzania. Informuje ona także o łącznej liczbie kopii zapasowych i archiwów w węźle magazynowania.

- **Panel Informacja**

  Zawiera szczegółowe informacje o wybranym węźle magazynowania i umożliwia zarządzanie zadaniem kompaktowania. Panel jest domyślnie zwinięty. Aby rozwinąć panel, należy kliknąć przycisk.  Zawartość panelu jest także zduplikowana w oknie **Storage node details** (s. 365) (Szczegóły węzła magazynowania).

Sposób pracy z węzłami magazynowania (typowy przepływ pracy)

1. Zainstaluj węzeł magazynowania Acronis Backup & Recovery 10.
2. Utwórz konto dla każdego użytkownika, któremu chcesz zezwolić na dostęp do węzła magazynowania.

   Uwaga: *Jeśli węzeł magazynowania i komputery użytkowników znajdują się w tej samej domenie usługi Active Directory, można pominąć ten krok.*

   Aby uzyskać informacje na temat uprawnień użytkownika w węźle magazynowania i w jego skarbcach zarządzanych, zobacz Uprawnienia użytkowników w węźle magazynowania (s. 90).
3. Dodaj (s. 364) węzeł magazynowania do serwera Acronis Backup & Recovery 10 Management Server.
4. Utwórz skarbiec zarządzany (s. 149): określ ścieżkę do skarbca, wybierz węzeł magazynowania, który będzie zarządzał skarbcem, a następnie wybierz operacje zarządzania, takie jak deduplikacja lub szyfrowanie.
5. Utwórz zasady tworzenia kopii zapasowych (s. 395) lub plan tworzenia kopii zapasowych, który będzie używał skarbca zarządzanego.

Czynności dotyczące węzłów magazynowania

Wszystkie opisane poniżej operacje wykonuje się poprzez kliknięcie odpowiednich elementów na pasku narzędzi zadań. Dostęp do operacji można także uzyskać poprzez pasek **Węzły magazynowania** (na panelu **Czynności i narzędzia**) i pozycję **Węzły magazynowania** w menu głównym.

Aby wykonać operację na węźle magazynowania dodanym do serwera zarządzania, wybierz najpierw węzeł magazynowania.

Poniżej przedstawiono wytyczne dotyczące wykonywania operacji na węzłach magazynowania.

Zadanie	Działanie
Dodaj węzeł magazynowania do serwera zarządzania	Kliknij **Dodaj**. W oknie Dodaj węzeł magazynowania (s. 364) określ komputer, na którym zainstalowany jest węzeł magazynowania. Dodanie węzła magazynowania powoduje ustanowienie relacji zaufania między serwerem zarządzania a węzłem magazynowania, tak samo jak w przypadku dodania komputerów do serwera. Po dodaniu węzła magazynowania do serwera zarządzania w węźle można tworzyć skarbce zarządzane.

Usuń węzeł magazynowania z serwera zarządzania	Kliknij **Usuń**. Po usunięciu węzła magazynowania z serwera zarządzania skarbce zarządzane przez węzeł magazynowania znikają z listy skarbców (s. 144) i nie są dostępne w celu wykonywania operacji. Wszystkie plany i zadania, które używają tych skarbców, zakończą się niepowodzeniem. Wszystkie bazy danych i skarbce tego węzła magazynowania pozostaną niezmienione. Wcześniej usunięty węzeł magazynowania można dodać ponownie do serwera zarządzania. W wyniku tego wszystkie skarbce zarządzane przez węzeł magazynowania pojawią się na liście skarbców i staną się ponownie dostępne dla wszystkich planów, które używają tych skarbców.
Utwórz centralny skarbiec zarządzany w wybranym węźle magazynowania	Kliknij **Utwórz skarbiec**. Zostanie otwarta strona Utwórz skarbiec zarządzany (s. 149) z wstępnie wybranym węzłem magazynowania. Wykonaj pozostałe kroki, aby utworzyć skarbiec.
Zmień harmonogram zadania kompaktowania	Po usunięciu kopii zapasowych ze skarbców deduplikacji (ręcznie lub podczas czyszczenia) w tych skarbcach i ich bazach danych mogą pojawić się dane bez odnośników. Procedura kompaktowania usuwa takie dane w celu zwolnienia miejsca. Dla każdego węzła magazynowania dostępne jest tylko jedno zadanie kompaktowania. Kliknij **Ponownie zaplanuj kompaktowanie**. W oknie **Harmonogram** skonfiguruj harmonogram procedury kompaktowania. Możliwe jest ustawienie tylko zdarzeń dotyczących czasu (harmonogramy: codziennie (s. 186), co tydzień (s. 188) i co miesiąc (s. 190)). Ustawienie wstępne to: Rozpocznij zadanie co **1 tydzień** w dniu tygodnia **Niedziela** o **03:00:00 . Powtórz raz**.
Wyświetl szczegóły węzła magazynowania	Kliknij **Wyświetl szczegóły**. W oknie **Storage node details** (s. 365) (Szczegóły węzła magazynowania) (jego zawartość jest także zduplikowana na panelu **Informacje**) sprawdź informacje dotyczące węzła magazynowania i skarbców zarządzanych przez ten węzeł. Można także zarządzać zadaniem kompaktowania, ręcznie uruchamiając i zatrzymując zadanie.
Odśwież listę węzłów magazynowania	Kliknij **Odśwież**. Konsola zarządzania zaktualizuje listę węzłów magazynowania z serwera zarządzania przy użyciu najnowszych informacji. Mimo że lista węzłów jest odświeżana automatycznie w oparciu o zdarzenia , dane mogą nie zostać pobrane natychmiast z serwera zarządzania ze względu na pewne opóźnienie. Po ręcznym odświeżeniu są wyświetlane najbardziej aktualne dane.

Dodawanie węzła magazynowania

Aby dodać węzeł magazynowania

1. W polu **Adres IP/nazwa** wprowadź nazwę lub adres IP komputera, na którym znajduje się węzeł magazynowania, bądź kliknij **Przeglądaj** i znajdź komputer w sieci.

   Jako nazwy węzła magazynowania użyj w pełni kwalifikowanej nazwy domeny (FQDN), to znaczy w pełni określonej nazwy domeny kończącej się domeną najwyższego poziomu. Nie należy wprowadzać ustawień „127.0.0.1” lub „localhost” jako adresu IP lub nazwy węzła magazynowania. Takie ustawienia nie są prawidłowe, nawet jeśli serwer zarządzania i węzeł magazynowania znajdują się na tym samym komputerze. Jest to spowodowane tym, że po

wdrożeniu zasad korzystających z węzła magazynowania każdy agent będzie próbował uzyskać dostęp do węzła magazynowania tak, jakby był on zainstalowany na hoście agenta.

2. Aby utworzyć prawidłowe konto użytkownika komputera, kliknij **Opcje>>** i określ:
   - **Nazwę użytkownika**. Wprowadzając nazwę konta użytkownika usługi Active Directory, należy również koniecznie określić nazwę domeny (DOMENA\Nazwa użytkownika lub Nazwaużytkownika@domena). Konto użytkownika musi być członkiem grupy administratorów komputera.
   - **Hasło**. Hasło dla konta.

   Zaznacz pole wyboru **Zapisz hasło**, aby przechować hasło konta.
3. Kliknij **OK**.

Rejestracja wymaga udziału węzła magazynowania, zatem nie może nastąpić, kiedy komputer jest w trybie offline.

Szczegóły węzła magazynowania

Na czterech kartach okna **Storage node details** (Szczegóły węzła magazynowania) znajdują się wszystkie informacje na temat wybranego węzła Acronis Backup & Recovery 10 Storage Node. Te informacje są także zduplikowane na panelu **Informacje**.

Właściwości węzła magazynowania

Na tej karcie są wyświetlane następujące informacje dotyczące wybranego węzła magazynowania:

- **Nazwa** — nazwa komputera, na którym zainstalowany jest węzeł magazynowania;
- **Adres IP** — adres IP komputera, na którym zainstalowany jest węzeł magazynowania;
- **Dostępność**:
  - **Nieznany** — status wyświetlany do momentu nawiązania pierwszego połączenia pomiędzy serwerem zarządzania a węzłem magazynowania po dodaniu węzła lub uruchomieniu usługi serwera zarządzania.
  - **Online** — węzeł magazynowania jest dostępny dla serwera zarządzania. To oznacza, że ostatnie połączenie serwera zarządzania z węzłem było udane. Nawiązanie połączenia następuje co 2 minuty.
  - **Offline** — węzeł magazynowania jest niedostępny.
  - **Wycofany** — węzeł magazynowania został zarejestrowany na innym serwerze zarządzania. To uniemożliwia sterowanie węzłem w obecnym serwerze.
- **Archiwa** — całkowita liczba archiwów przechowywanych we wszystkich skarbcach zarządzanych przez węzeł magazynowania;
- **Kopie zapasowe** — całkowita liczba kopii zapasowych przechowywanych w archiwach w skarbcach zarządzanych przez węzeł magazynowania.

Skarbce

Na tej karcie jest wyświetlana lista skarbców zarządzanych przez węzeł magazynowania.

Aby otworzyć skarbiec zarządzany w celu sprawdzenia szczegółów lub przeprowadzenia na nim operacji, wybierz skarbiec, a następnie kliknij **Pokaż skarbiec** (na pasku narzędzi karty). W widoku **Skarbiec centralny** (s. 145) wykonaj wymagane czynności.

Usługi

Na tej karcie są wyświetlane parametry planowania zadania kompaktowania.

Zadania usługi

Na tej karcie administrator serwera zarządza zadaniem kompaktowania i sprawdza jego parametry. W węźle magazynowania może występować tylko jedno zadanie kompaktowania.

7.1.6 Zadania

Widok **Zadania** umożliwia monitorowanie zadań istniejących na zarejestrowanych komputerach i zarządzanie nimi. Użytkownik może wyświetlać szczegóły zadań, ich stany oraz wyniki wykonywania, a także uruchamiać, zatrzymywać i usuwać zadania.

Aby dowiedzieć się, co aktualnie robi zadanie na komputerze, należy sprawdzić stan wykonywania zadania. Status zadania ułatwia oszacowanie, czy zadanie jest wykonywane pomyślnie.

Aby dowiedzieć się więcej o stanach i statusach zadania, zobacz sekcje Stany zadania (s. 207) i Statusy zadania (s. 208).

Sposób pracy z zadaniami

- Użyj funkcji filtrowania i sortowania (s. 368) w celu wyświetlenia żądanych zadań w tabeli.
- Wybierz zadanie i wykonaj odpowiednią czynność.

Czynności dotyczące zadań

Poniżej przedstawiono wskazówki dotyczące wykonywania operacji na zadaniach.

Zadanie	Czynności
Utworzenie nowego planu lub zadania tworzenia kopii zapasowych na zarejestrowanym komputerze	Kliknij **Nowy** i wybierz jedną z następujących opcji: ▪ Plan tworzenia kopii zapasowych (s. 219) ▪ Zadanie odzyskiwania ▪ Zadanie sprawdzania poprawności (s. 271) Następnie określ zarejestrowany komputer, na którym zostanie uruchomione wybrane zadanie lub wybrany plan tworzenia kopii zapasowych.
Wyświetlanie szczegółów zadania	Kliknij **Wyświetl szczegóły**. W oknie Szczegółowe informacje na temat zadania (s. 213) zapoznaj się ze wszystkimi informacjami dotyczącymi wybranego zadania.
Wyświetlanie dziennika zadania	Kliknij **Wyświetl dziennik**. Widok Dziennik (s. 368) przedstawi listę wszystkich wpisów w dzienniku związanych z wybranym zadaniem.
Uruchomienie zadania	Kliknij **Uruchom**. Zadanie zostanie wykonane natychmiast, niezależnie od harmonogramu.

Zatrzymanie zadania	Kliknij **Zatrzymaj**. *Co się stanie, jeśli zatrzymam zadanie?* Ogólnie rzecz biorąc, zatrzymanie zadania spowoduje przerwanie jego operacji (tworzenia kopii zapasowej, odzyskiwania, sprawdzania poprawności, eksportowania, konwersji, migracji). Zadanie przejdzie najpierw w stan **Zatrzymywane,** a następnie w stan Bezczynne. Ewentualny harmonogram zadania pozostanie ważny. Aby dokończyć operację, trzeba będzie uruchomić zadanie od początku. ▪ **Zadanie odzyskiwania (z kopii zapasowej dysku):** wolumin docelowy zostanie usunięty, a jego miejsce stanie się nieprzydzielone — tak samo jak w przypadku niepowodzenia odzyskiwania. Aby odzyskać „utracony" wolumin, należy ponownie uruchomić zadanie. ▪ **Zadanie odzyskiwania (z kopii zapasowej plików):** przerwana operacja może spowodować zmiany w folderze docelowym. W zależności od tego, w jakim okresie zadanie zostało zatrzymane, niektóre pliki mogą zostać odzyskane, a inne nie. Aby odzyskać wszystkie pliki, należy ponownie uruchomić zadanie.
Edycja zadania	Kliknij **Edytuj**. *Dlaczego nie mogę edytować zadania?* ▪ **Zadanie należy do planu tworzenia kopii zapasowych.** Bezpośrednia edycja jest możliwa tylko w przypadku zadań, które nie należą do planu tworzenia kopii zapasowych, takich jak zadanie odzyskiwania. Jeśli zmian wymaga zadanie należące do lokalnego planu tworzenia kopii zapasowych, należy zmodyfikować ten plan. Zadanie należące do scentralizowanego planu tworzenia kopii zapasowych można zmodyfikować przez edycję scentralizowanych zasad będących źródłem tego planu. Może to zrobić tylko administrator serwera zarządzania. ▪ **Brak odpowiednich uprawnień.** Jeśli użytkownik nie ma na komputerze uprawnień administratora, nie może modyfikować zadań należących do innych użytkowników.
Usunięcie zadania	Kliknij **Usuń**. *Dlaczego nie mogę usunąć zadania?* ▪ **Zadanie należy do planu tworzenia kopii zapasowych.** Zadania należącego do planu tworzenia kopii zapasowych nie można usunąć w oderwaniu od planu. Zmodyfikuj plan tak, aby usunąć z niego zadanie, lub usuń cały plan. ▪ **Brak odpowiednich uprawnień.** Jeśli użytkownik nie ma na komputerze uprawnień administratora, nie może usuwać zadań należących do innych użytkowników. ▪ **Jest to wbudowane zadanie kompaktowania.** Każdy węzeł magazynowania ma wbudowanie zadanie obsługi zwane zadaniem kompaktowania. Nie można go usunąć.

Odświeżenie tabeli zadań	Kliknij **Odśwież**. Konsola zarządzania zaktualizuje listę zadań istniejących na komputerze z uwzględnieniem najnowszych informacji Mimo że lista zadań jest odświeżana automatycznie na podstawie zdarzeń, ze względu na pewne opóźnienie dane z komputera zarządzanego mogą nie pojawić się natychmiast. Po ręcznym odświeżeniu wyświetlane są najbardziej aktualne dane.

Zadania filtrowania i sortowania

Poniżej przedstawiono wytyczne dotyczące filtrowania i sortowania zadań.

Zadanie	Działanie
Ustaw liczbę wyświetlanych zadań	Wybierz kolejno **Opcje > Opcje konsoli > Liczba zadań** (s. 100) i ustaw żądaną wartość. Maksymalnie można wyświetlić 500 zadań. Jeśli liczba zadań przekracza określoną wartość, użyj filtrów, aby wyświetlić dodatkowe zadania.
Sortuj zadania według kolumny	Kliknij nagłówek kolumny, aby posortować zadania w porządku rosnącym. Kliknij ponownie nagłówek kolumny, aby posortować zadania w porządku malejącym.
Filtruj zadania według nazwy, właściciela lub planu tworzenia kopii zapasowych	Wpisz nazwę zadania (lub nazwę właściciela albo nazwę planu tworzenia kopii zapasowych) w polu pod odpowiednim nagłówkiem kolumny. Zostanie wyświetlona lista zadań, których nazwy (lub nazwy właściciela albo nazwy planu tworzenia kopii zapasowych) są całkowicie lub częściowo zgodne z wprowadzoną wartością.
Filtruj zadania według typu, stanu wykonania, stanu, typu, pochodzenia, ostatniego wyniku lub harmonogramu	W polu pod odpowiednim nagłówkiem wybierz żądaną wartość z listy.

Konfigurowanie tabeli zadań

Domyślnie w tabeli jest wyświetlanych osiem kolumn, a pozostałe są ukryte. W razie potrzeby można ukryć wyświetlane kolumny i wyświetlić ukryte kolumny.

Aby wyświetlić lub ukryć kolumny

1. Kliknij prawym przyciskiem myszy nagłówek kolumny, aby wyświetlić menu kontekstowe. Zaznaczone elementy menu odpowiadają nagłówkom kolumn wyświetlanych w tabeli.
2. Kliknij elementy, które chcesz wyświetlić/ukryć.

7.1.7 Dziennik

W dzienniku programu Acronis Backup & Recovery 10 jest przechowywana historia czynności wykonywanych przez oprogramowanie na komputerze lub czynności wykonywanych przez użytkownika na komputerze przy użyciu oprogramowania. Gdy użytkownik na przykład edytuje zadanie, do dziennika jest dodawany wpis. Gdy oprogramowanie wykonuje zadanie, dodaje wiele wpisów informujących o aktualnie wykonywanych czynnościach.

Rejestrowanie lokalne i centralne w programie Acronis Backup & Recovery 10

Program Acronis Backup & Recovery 10 ma lokalny i centralny dziennik zdarzeń.

Lokalny dziennik zdarzeń

W lokalnym dzienniku zdarzeń znajdują się informacje na temat operacji programu Acronis Backup & Recovery 10 na komputerze zarządzanym. Na przykład utworzenie planu tworzenia kopii zapasowych, wykonanie planu tworzenia kopii zapasowych, zarządzanie archiwami w skarbcach osobistych, czy wykonanie zadania odzyskiwania, spowoduje zarejestrowanie zdarzenia w lokalnym dzienniku zdarzeń. Fizycznie jest to zbiór plików XML zapisanych w komputerze. Dostęp do lokalnego dziennika zdarzeń zarządzanego komputera można uzyskać, gdy konsola jest połączona z komputerem. Nie można wyłączyć lokalnego rejestrowania zdarzeń.

Operacje wykonane przy użyciu nośnika startowego są również rejestrowane, ale czas istnienia dziennika jest ograniczony tylko do bieżącej sesji. Ponowne uruchomienie powoduje skasowanie dziennika, ale można go zapisać w pliku, jeśli komputer jest uruchomiany z nośnika.

Węzeł magazynowania Acronis Backup & Recovery 10 Storage Node ma własny lokalny dziennik zdarzeń. Zdarzenia w tym dzienniku są dostępne tylko poprzez dziennik centralny.

Centralny dziennik zdarzeń

Sposób pracy z wpisami dziennika

- Maksymalna liczba wpisów przechowywanych w dzienniku centralnym wynosi 50 000. Maksymalna liczba wpisów, które mogą być wyświetlane, wynosi 10 000. Gdy liczba wpisów dziennika jest większa niż 10 000, należy użyć funkcji filtrowania i sortowania, aby wyświetlić żądane wpisy dziennika w tabeli. Użytkownik może także ukrywać niepotrzebne kolumny i wyświetlać ukryte. Aby uzyskać szczegółowe informacje, zapoznaj się z sekcją Filtrowanie i sortowanie wpisów dziennika (s. 370).
- Wybierz wpis dziennika (lub wpisy dziennika), aby wykonać odpowiednią czynność. Aby uzyskać szczegółowe informacje, zobacz Czynności dotyczące wpisów dziennika (s. 370).
- Panel **Informacja** służy do przeglądania szczegółowych informacji na temat wybranego wpisu dziennika. Panel jest domyślnie zwinięty. Aby rozwinąć panel, należy kliknąć przycisk. Zawartość panelu jest także zduplikowana w oknie **Szczegóły wpisu dziennika** (s. 371).

Sposoby otwierania widoku „Dziennik" zawierającego wstępnie odfiltrowane wpisy dziennika

Po wybraniu elementów w innych widokach administracyjnych (Pulpit nawigacyjny, Komputery, Zasady tworzenia kopii zapasowych, Zadania) można wyświetlić widok Dziennik, zawierający wpisy przefiltrowane pod kątem sprawdzanego elementu. Dlatego nie trzeba samemu konfigurować filtrów w tabeli dziennika.

Widok	Czynność
Pulpit nawigacyjny	Kliknij prawym przyciskiem myszy dowolną podświetloną datę w kalendarzu i wybierz **Wyświetl dziennik**. Wyświetlony widok Dziennik będzie zawierał listę wpisów przefiltrowaną według wybranej daty.
Komputery	Wybierz komputer lub grupę komputerów i kliknij **Wyświetl dziennik**. Wyświetlony widok Dziennik będzie zawierał listę wpisów związanych z wybranym komputerem lub grupą.
Zasady tworzenia kopii zapasowych	Wybierz zasadę tworzenia kopii zapasowych i kliknij **Wyświetl dziennik**. Wyświetlony widok Dziennik będzie zawierał listę wpisów związanych z wybraną zasadą.
Zadania	Wybierz zadanie i kliknij **Wyświetl dziennik**. Wyświetlony widok Dziennik będzie zawierał listę wpisów należących do wybranego zadania.

Czynności dotyczące wpisów dziennika

Wszystkie opisane poniżej operacje wykonuje się, klikając odpowiednie elementy na **pasku narzędzi** dziennika. Wszystkie te operacje można również wykonać za pomocą menu kontekstowego (klikając prawym przyciskiem myszy wpis dziennika) lub za pomocą paska **Log actions** (Czynności dotyczące dziennika) (w panelu **Czynności i narzędzia**).

Poniżej przedstawiono wytyczne dotyczące wykonywania czynności związanych z wpisami dziennika.

Zadanie	Działanie
Wybierz pojedynczy wpis dziennika	Kliknij wpis.
Wybierz wiele wpisów dziennika	▪ *Niesąsiadujące*: przytrzymaj naciśnięty klawisz **CTRL** i kliknij pojedynczo wpisy dziennika. ▪ *Sąsiadujące*: wybierz pojedynczy wpis dziennika, a następnie przytrzymaj naciśnięty klawisz **SHIFT** i kliknij inny wpis. Wszystkie wpisy między pierwszym a ostatnim zaznaczeniem także zostaną zaznaczone.
Wyświetl szczegółowe informacje o wpisie dziennika	1. Wybierz wpis dziennika. 2. Wykonaj jedną z następujących czynności: ▪ Kliknij **Wyświetl szczegóły**. W oddzielnym oknie zostaną wyświetlone szczegółowe informacje o wpisie dziennika. ▪ Rozwiń panel Informacja, klikając przycisk.
Zapisz wybrane wpisy dziennika w pliku	1. Zaznacz pojedynczy wpis dziennika lub wiele wpisów dziennika. 2. Kliknij **Zapisz zaznaczone w pliku**. 3. W otwartym oknie określ ścieżkę i nazwę pliku.
Zapisz wszystkie wpisy dziennika w pliku	1. Upewnij się, że nie są ustawione żadne filtry. 2. Kliknij **Zapisz wszystko w pliku**. 3. W otwartym oknie określ ścieżkę i nazwę pliku.
Zapisz wszystkie odfiltrowane wpisy dziennika w pliku	1. Ustaw filtry tak, aby uzyskać listę wpisów dziennika spełniających kryteria filtrowania. 2. Kliknij **Zapisz wszystko w pliku**. 3. W otwartym oknie określ ścieżkę i nazwę pliku. Wpisy dziennika z tej listy zostaną zapisane.
Usuń wszystkie wpisy dziennika	Kliknij **Wyczyść dziennik**. Wszystkie wpisy dziennika zostaną usunięte z dziennika i zostanie utworzony nowy wpis dziennika. Będzie on zawierał informacje o tym, kto i kiedy usunął wpisy.
Konfiguruj poziom rejestrowania	Kliknij **Konfiguruj poziom rejestrowania**. W oknie **Poziom rejestrowania** (s. 101) określ, czy zdarzenia zapisane w dziennikach zarejestrowanych komputerów mają być zbierane w dzienniku centralnym.

Filtrowanie i sortowanie wpisów dziennika

Poniżej przedstawiono wytyczne dotyczące filtrowania i sortowania wpisów dziennika.

Zadanie	Działanie
Wyświetl wpisy dziennika dotyczące określonego przedziału czasu	1. W polu **Od** wybierz datę, od której mają być wyświetlane wpisy dziennika. 2. W polu **Do** wybierz datę, do której mają być wyświetlane wpisy dziennika.
Filtruj wpisy dziennika według typu	Naciśnij lub zwolnij następujące przyciski paska narzędzi:  aby filtrować komunikaty o błędach,  aby filtrować komunikaty ostrzegawcze,  aby filtrować komunikaty informacyjne.
Filtruj wpisy dziennika według oryginalnego planu tworzenia kopii zapasowych lub typu jednostki zarządzanej	W kolumnie **Plan tworzenia kopii zapasowych** (lub **Typ jednostki zarządzanej**) wybierz z listy plan tworzenia kopii zapasowych lub typ jednostki zarządzanej.
Filtruj wpisy dziennika według zadania, jednostki zarządzanej, komputera, kodu, właściciela	W polu pod odpowiednim nagłówkiem kolumny wpisz wymaganą wartość (nazwę zadania, nazwę komputera, nazwę właściciela itp.). Zostanie wyświetlona lista wpisów dziennika, które całkowicie lub częściowo zgadzają się z wprowadzoną wartością.
Sortuj wpisy dziennika według daty i godziny	Kliknij nagłówek kolumny, aby posortować wpisy dziennika w porządku rosnącym. Kliknij go ponownie, aby posortować wpisy dziennika w porządku malejącym.

Konfigurowanie tabeli dziennika

Domyślnie w tabeli jest wyświetlanych siedem kolumn, a pozostałe są ukryte. W razie potrzeby można ukryć wyświetlane kolumny i wyświetlić ukryte kolumny.

Aby wyświetlić lub ukryć kolumny

1. Kliknij prawym przyciskiem myszy nagłówek kolumny, aby wyświetlić menu kontekstowe. Zaznaczone elementy menu odpowiadają nagłówkom kolumn wyświetlanych w tabeli.
2. Kliknij elementy, które chcesz wyświetlić/ukryć.

Szczegóły wpisu scentralizowanego dziennika

Wyświetlane są szczegółowe informacje dotyczące wpisu dziennika. Informacje te można skopiować do schowka.

Aby skopiować szczegółowe informacje, kliknij przycisk **Kopiuj do schowka**.

Pola danych wpisu dziennika

Wpis scentralizowanego dziennika zawiera następujące pola danych:

- **Typ** — typ zdarzenia (Błąd, Ostrzeżenie, Informacja);
- **Data** — data i godzina wystąpienia zdarzenia;
- **Zasady** — zasady tworzenia kopii zapasowych, z którymi związane jest zdarzenie (jeśli dotyczą);
- **Zadanie** — zadanie, z którym związane jest zdarzenie (jeśli dotyczy);
- **Typ jednostki zarządzanej** — typ jednostki zarządzanej, w której wystąpiło zdarzenie (jeśli dotyczy);
- **Jednostka zarządzana** — nazwa jednostki zarządzanej, w której wystąpiło zdarzenie (jeśli dotyczy);

- **Komputer** — nazwa komputera, na którym wystąpiło zdarzenie (jeśli dotyczy);
- **Kod** — puste pole lub kod błędu programu, jeśli typem zdarzenia jest błąd. Kod błędu to liczba całkowita, która może zostać użyta przez usługę pomocy technicznej Acronis w celu rozwiązania problemu;
- **Moduł** — puste pole lub numer modułu programu, w którym wystąpił błąd. Jest to liczba całkowita, która może zostać użyta przez usługę pomocy technicznej Acronis w celu rozwiązania problemu;
- **Właściciel** — nazwa użytkownika będącego właścicielem (s. 35) zasad/planu tworzenia kopii zapasowych;
- **Komunikat** — tekstowy opis zdarzenia.

Kopiowane szczegóły wpisu dziennika będą miały następujący wygląd:

```
---------------------------Szczegóły wpisu dziennika---------------------------
Typ:                                Informacja
Data i godzina:                     DD.MM.RRRR HH:MM:SS
Plan tworzenia kopii zapasowych:    Nazwa planu tworzenia kopii zapasowych
Zadanie:                            Nazwa zadania
Typ jednostki zarządzanej:          Komputer
Jednostka zarządzana:               NAZWA_JEDNOSTKI
Komputer:                           NAZWA_KOMPUTERA
Komunikat:
Opis operacji
Kod:                                12(3x45678A)
Moduł:                              Nazwa modułu
Właściciel:                         Właściciel planu
-------------------------------------------------------------------------------
```

7.1.8 Raporty

Dzięki raportom administrator serwera zarządzania może uzyskać dokładne, uporządkowane informacje na temat operacji związanych z ochroną danych w przedsiębiorstwie. Raporty mogą być instrumentem dokładnej analizy całej infrastruktury kopii zapasowych w sieci firmowej.

Raporty są tworzone przez serwer zarządzania na podstawie statystyk i dzienników zebranych z zarejestrowanych komputerów i przechowywanych w specjalnych bazach danych.

Raporty są generowane na podstawie szablonów raportów. Szablony definiują informacje uwzględniane w raporcie i sposób ich prezentacji.

Serwer zarządzania Acronis Backup & Recovery 10 Management Server oferuje następujące typy szablonów raportów:

- Zarejestrowane komputery
- Zasady tworzenia kopii zapasowych istniejące na serwerze zarządzania
- Lokalne i scentralizowane plany tworzenia kopii zapasowych istniejące na zarejestrowanych komputerach
- Lokalne i scentralizowane zadania istniejące na zarejestrowanych komputerach
- Archiwa i kopie zapasowe przechowywane w centralnych skarbcach zarządzanych
- Statystyki centralnego skarbca zarządzanego
- Historia działań dotyczących zadań

Raporty o komputerach, zasadach i planach tworzenia kopii zapasowych, zadaniach oraz archiwach i kopiach zapasowych są aktualizowane na bieżąco.

Raporty o statystykach skarbców i działaniach dotyczących zadań są tworzone dla określonych przedziałów czasu i przedstawiają odpowiadające im informacje historyczne. Przedziały mogą wynosić od kilku dni do kilku lat, w zależności od ilości danych przechowywanych w bazach.

Generowanie raportów

Aby rozpocząć generowanie raportu, wybierz szablon raportu w widoku **Raporty** i kliknij **Wygeneruj** na pasku narzędzi.

Istnieją dwa typy szablonów raportów: niestandardowe i wstępnie zdefiniowane. W szablonie niestandardowym można za pomocą filtrów określić pozycje uwzględniane w raporcie. Wstępnie zdefiniowany szablon raportu pozwala na utworzenie raportu za pomocą jednego kliknięcia myszą.

Raport będzie zawierać informacje wybrane, pogrupowane i posortowane zgodnie z ustawieniami szablonu. Raport jest wyświetlany w oddzielnym interaktywnym oknie, które umożliwia rozwijanie i zwijanie tabel. Raport można wyeksportować do pliku XML i otworzyć go później w programie Microsoft Word albo Microsoft Excel.

Raporty o komputerach

W tym widoku można wygenerować raport o komputerach, które są zarejestrowane na serwerze zarządzania. Raport składa się z przynajmniej jednej tabeli.

Filtry

W sekcji **Filtry** wybierz komputery, które chcesz uwzględnić w raporcie. W raporcie znajdą się tylko komputery spełniające wszystkie kryteria filtru.

- **Komputery** — lista komputerów. Wybierz komputery fizyczne lub maszyny wirtualne.
- **Stan** — stany komputerów: **OK**, **Ostrzeżenie** i/lub **Błąd**.
- **Ostatnie połączenie** (tylko komputery fizyczne) — okres ostatniego połączenia między komputerami i serwerem zarządzania.
- **Ostatnia pomyślnie utworzona kopia zapasowa** — okres ostatniej pomyślnie utworzonej kopii zapasowej na każdym z komputerów.
- **Następna kopia zapasowa** — okres uruchomienia następnej zaplanowanej operacji tworzenia kopii zapasowej na każdym z komputerów.
- **System operacyjny** — systemy operacyjne działające na komputerach.
- **Adres IP** (tylko komputery fizyczne) — zakres ostatnio uzyskanych adresów IP komputerów.
- **Dostępność** (tylko komputery fizyczne) — typy dostępności komputerów: **Online** lub **Offline**.

Przy domyślnych ustawieniach filtru raport obejmie wszystkie komputery fizyczne.

Widok raportu

W sekcji **Widok raportu** wybierz wygląd raportu:

- Określ, czy wszystkie elementy mają być wyświetlane w jednej tabeli, czy mają być pogrupowane według określonej kolumny.
- Określ wyświetlane kolumny tabeli i ich kolejność.
- Określ sposób sortowania tabeli.

Raport o zasadach tworzenia kopii zapasowych

W tym widoku można wygenerować raport o istniejących na serwerze zarządzania zasadach tworzenia kopii zapasowych. Raport składa się z przynajmniej jednej tabeli.

Filtry

W sekcji **Filtry** wybierz zasady tworzenia kopii zapasowych, które chcesz uwzględnić w raporcie. W raporcie znajdą się tylko zasady spełniające wszystkie kryteria filtru.

- **Zasady tworzenia kopii zapasowych** — lista zasad tworzenia kopii zapasowych.
- **Typ źródła** — typ danych umieszczanych w kopiach zapasowych na podstawie zasad tworzenia kopii: **Dyski/woluminy** i/lub **Pliki**.
- **Stan wdrażania** — stan wdrażania zasad tworzenia kopii zapasowych, na przykład **Wdrożone**.
- **Stan** — statusy zasad tworzenia kopii zapasowych: **OK**, **Ostrzeżenie** i/lub **Błąd**.
- **Harmonogram** — typy harmonogramów zasad tworzenia kopii zapasowych: **Ręczne** i/lub **Zaplanowane**. Harmonogram ręczny oznacza, że odpowiedni centralny plan tworzenia kopii zapasowych jest wykonywany dopiero po ręcznym uruchomieniu.
- **Właściciel** — lista użytkowników, którzy utworzyli zasady tworzenia kopii zapasowych.

Przy domyślnych ustawieniach filtru raport obejmie wszystkie zasady tworzenia kopii zapasowych.

Widok raportu

W sekcji **Widok raportu** wybierz wygląd raportu:

- Określ, czy wszystkie elementy mają być wyświetlane w jednej tabeli, czy mają być pogrupowane według określonej kolumny.
- Określ wyświetlane kolumny tabeli i ich kolejność.
- Określ sposób sortowania tabeli.

Raport o planach tworzenia kopii zapasowych

W tym widoku można wygenerować raport o planach tworzenia kopii zapasowych, które istnieją na zarejestrowanych komputerach. Raport składa się z przynajmniej jednej tabeli.

Filtry

W sekcji **Filtry** wybierz plany tworzenia kopii zapasowych, które chcesz uwzględnić w raporcie. W raporcie znajdą się tylko plany spełniające wszystkie kryteria filtru.

- **Początek** — typy pochodzenia planów tworzenia kopii zapasowych: **Lokalny** i/lub **Centralny**.
- **Zasady tworzenia kopii zapasowych** (dostępne tylko dla scentralizowanych planów tworzenia kopii zapasowych) — zasady tworzenia kopii zapasowych, na których są oparte scentralizowane plany tworzenia kopii.
- **Komputery** — lista komputerów, na których istnieją plany tworzenia kopii zapasowych.
- **Stan wykonania** — stany wykonania planów, na przykład **Uruchomione**.
- **Stan** — statusy planów tworzenia kopii zapasowych: **OK**, **Ostrzeżenie** i/lub **Błąd**.
- **Godzina ostatniego zakończenia** — okres ostatnio utworzonej kopii zapasowej w ramach każdego z planów.
- **Harmonogram** — typy harmonogramów planów tworzenia kopii zapasowych: **Ręczne** i/lub **Zaplanowane**. Harmonogram ręczny oznacza, że plan tworzenia kopii zapasowych jest wykonywany dopiero po ręcznym uruchomieniu.
- **Właściciel** — lista użytkowników, którzy utworzyli plany tworzenia kopii zapasowych.

Przy domyślnych ustawieniach filtru raport obejmie wszystkie plany tworzenia kopii zapasowych ze wszystkich komputerów.

Widok raportu

W sekcji **Widok raportu** wybierz wygląd raportu:

- Określ, czy wszystkie elementy mają być wyświetlane w jednej tabeli, czy mają być pogrupowane według określonej kolumny.
- Określ wyświetlane kolumny tabeli i ich kolejność.
- Określ sposób sortowania tabeli.

Raport o zadaniach

W tym widoku można wygenerować raport o zadaniach uruchomionych na zarejestrowanych komputerach. Raport składa się z przynajmniej jednej tabeli.

Filtry

W sekcji **Filtry** wybierz zadania, które chcesz uwzględnić w raporcie. W raporcie znajdą się tylko zadania spełniające wszystkie kryteria filtru.

- **Początek** — typy pochodzenia zadań: **Centralny**, **Lokalny** i/lub **Lokalny bez planu tworzenia kopii zapasowych**. Zadanie centralne należy do scentralizowanego planu tworzenia kopii zapasowych. Zadanie lokalne może nie należeć do planu tworzenia kopii zapasowych (na przykład zadanie odzyskiwania).
- **Zasady tworzenia kopii zapasowych** (tylko zadania centralne) — zasady tworzenia kopii zapasowych, na których są oparte zadania.
- **Komputery** — lista komputerów, na których istnieją zadania.
- **Typ** — typy zadań, na przykład zadania tworzenia kopii zapasowych.
- **Stan wykonania** — stany wykonania zadań, na przykład **Uruchomione**.
- **Ostatni wynik** — ostatnie wyniki zadań: **Wykonane pomyślnie**, **Wykonane pomyślnie z ostrzeżeniami** i/lub **Zakończone niepowodzeniem**.
- **Harmonogram** — typy harmonogramów zadań: **Ręczne** lub **Zaplanowane**. Harmonogram ręczny oznacza, że zadanie jest wykonywane dopiero po ręcznym uruchomieniu.
- **Właściciel** — lista użytkowników, którzy utworzyli zadania.
- **Czas trwania** — długość ostatniego wykonywania poszczególnych zadań.

Przy domyślnych ustawieniach filtru raport obejmie wszystkie zadania ze wszystkich komputerów.

Widok raportu

W sekcji **Widok raportu** wybierz wygląd raportu:

- Określ, czy wszystkie elementy mają być wyświetlane w jednej tabeli, czy mają być pogrupowane według określonej kolumny.
- Określ wyświetlane kolumny tabeli i ich kolejność.
- Określ sposób sortowania tabeli.

Raport o archiwach i kopiach zapasowych

W tym widoku można wygenerować raport o archiwach przechowywanych w zarządzanych skarbcach centralnych. Raport składa się z przynajmniej jednej tabeli.

Filtry

W sekcji **Filtry** wybierz archiwa, które chcesz uwzględnić w raporcie. W raporcie znajdą się tylko archiwa spełniające wszystkie kryteria filtru.

- **Skarbce** — lista zarządzanych skarbców centralnych, w których przechowywane są archiwa.
- **Komputery** — lista zarejestrowanych komputerów, z których utworzono archiwa.
- **Typ** — typy archiwów: na poziomie dysku i/lub na poziomie pliku.
- **Właściciel** — lista użytkowników, którzy utworzyli archiwa.
- **Godzina utworzenia** — okres utworzenia ostatniej kopii zapasowej w każdym z archiwów.
- **Zajęte miejsce** — limity miejsca zajmowanego przez każde z archiwów.
- **Dane uwzględnione w kopii zapasowej** — limity łącznego rozmiaru danych przechowywanych aktualnie w każdym z archiwów. Rozmiar ten może odbiegać od zajętego miejsca z powodu kompresji lub deduplikacji.
- **Liczba kopii zapasowych** — limit liczby kopii zapasowych znajdujących się w każdym archiwum.

Przy domyślnych ustawieniach filtru raport obejmie wszystkie archiwa przechowywane w zarządzanych skarbcach centralnych.

Widok raportu

W sekcji **Widok raportu** wybierz wygląd raportu:

- Określ, czy wszystkie elementy mają być wyświetlane w jednej tabeli, czy mają być pogrupowane według określonej kolumny.
- Określ wyświetlane kolumny tabeli i ich kolejność.
- Określ sposób sortowania tabeli.

Raporty o statystykach skarbców

W tym widoku można wygenerować raport o wykorzystaniu centralnych skarbców zarządzanych, które są obecnie dodane do serwera zarządzania. Raport składa się z przynajmniej jednej tabeli i diagramu.

Zakres raportu

W sekcji **Zakres raportu** wybierz przedział czasu, dla którego chcesz wygenerować raport. W raporcie wyświetlany jest stan wybranych skarbców o podanej porze każdego dnia okresu uwzględnionego w raporcie.

Filtry

W sekcji **Filtry** wybierz centralne skarbce zarządzane, które chcesz uwzględnić w raporcie, oraz określ, czy chcesz utworzyć podsumowanie dotyczące wszystkich wybranych skarbców.

Podsumowanie przedstawia łączną ilość wolnego i zajętego miejsca, łączną ilość danych w kopiach zapasowych, łączną liczbę archiwów i kopii zapasowych oraz średnie wartości wskaźników w wybranych skarbcach.

Przy domyślnych ustawieniach filtru raport obejmie informacje o wszystkich centralnych skarbcach zarządzanych oraz podsumowanie.

Widok raportu

W sekcji **Widok raportu** wybierz wygląd raportu:

- Określ wyświetlane kolumny tabeli i ich kolejność.
- Wybierz diagramy do uwzględnienia w raporcie. Diagramy przedstawiają poziom wykorzystania miejsca w skarbcach.

Raport o działaniach dotyczących zadań

W tym widoku można wygenerować raport o zadaniach istniejących na zarejestrowanych komputerach w wybranym okresie. Raport składa się z przynajmniej jednego diagramu. Jeden diagram odpowiada jednemu komputerowi.

Diagramy przedstawiają, ile razy poszczególne zadania zostały wykonane określonego dnia z każdym z następujących wyników: „Wykonane pomyślnie”, „Wykonane pomyślnie z ostrzeżeniami” i „Zakończone niepowodzeniem”.

Zakres raportu

W sekcji **Zakres raportu** wybierz przedział czasu, dla którego chcesz wygenerować raport.

Filtry

W sekcji **Filtry** wybierz zadania, które chcesz uwzględnić w raporcie. W raporcie znajdą się tylko zadania spełniające wszystkie kryteria filtru.

- **Początek** — typy pochodzenia zadań: **Centralny**, **Lokalny** i/lub **Lokalny bez planu tworzenia kopii zapasowych**. Zadanie centralne należy do scentralizowanego planu tworzenia kopii zapasowych. Zadanie lokalne może nie należeć do planu tworzenia kopii zapasowych (na przykład zadanie odzyskiwania).
- **Zasady tworzenia kopii zapasowych** (tylko zadania centralne) — zasady tworzenia kopii zapasowych, na których są oparte zadania. Ustawienie domyślne oznacza wszystkie zasady tworzenia kopii zapasowych, które kiedykolwiek istniały w okresie uwzględnionym w raporcie.
- **Komputery** — lista komputerów, na których istnieją zadania.
- **Typ** — typy zadań, na przykład zadania tworzenia kopii zapasowych.
- **Właściciel** — lista użytkowników, którzy utworzyli zadania.

Przy domyślnych ustawieniach filtru raport obejmie wszystkie zadania, które kiedykolwiek istniały na zarejestrowanych komputerach w okresie uwzględnionym w raporcie.

Wybór kolumn

W oknie **Wybór kolumn** można wybrać kolumny do uwzględnienia w raporcie i określić ich kolejność.

Kolumny zawarte w tabelach raportu (od lewej do prawej strony) będą zgodne z listą w sekcji **Wyświetl w raporcie**. Najwyższa kolumna na liście znajdzie się po lewej stronie raportu.

Podczas wybierania wyświetlanych kolumn przyciski strzałek w lewo i w prawo służą odpowiednio do uwzględniania i wykluczania kolumn, a przyciski strzałek w górę i w dół — do zmiany ich kolejności.

Niektórych kolumn — na przykład **Nazwa komputera** w raporcie o komputerach — nie można wykluczyć z listy ani przesuwać w górę lub w dół.

Widok raportu

Aby przeglądarka internetowa mogła prawidłowo wyświetlać daty i inne informacje z generowanych raportów, włącz obsługę zawartości aktywnej (JavaScript). Możesz ją włączyć tylko dla obecnie wyświetlanej strony lub na stałe. Aby umożliwić tymczasową obsługę zawartości aktywnej w przeglądarce Internet Explorer, kliknij pasek Informacje wyświetlany u góry strony i kliknij **Zezwalaj na zablokowaną zawartość**.

Aby trwale włączyć zawartość aktywną

W przeglądarce Internet Explorer

1. W menu **Narzędzia** kliknij **Opcje internetowe**, a następnie kliknij kartę **Zaawansowane**.
2. W sekcji **Zabezpieczenia** zaznacz pole wyboru **Zezwalaj zawartości aktywnej na działanie w plikach na moim komputerze**.
3. Kliknij **OK**.

W przeglądarce Mozilla Firefox

1. W menu **Opcje** kliknij **Treść**.
2. Sprawdź, czy pole wyboru **Włącz obsługę języka JavaScript** jest zaznaczone.
3. Kliknij **OK**.

7.2 Konfigurowanie komponentów programu Acronis Backup & Recovery 10

W systemie Windows różne parametry komponentów programu Acronis Backup & Recovery 10 można skonfigurować na trzy sposoby:

- przy użyciu szablonu administracyjnego Acronis Administrative Template;
- przy użyciu graficznego interfejsu użytkownika,
- przez modyfikację rejestru systemu Windows.

W systemie Linux szablon administracyjny i rejestr nie są używane. Parametry konfiguruje się przez edycję odpowiednich plików konfiguracyjnych.

Jeśli wartości dowolnego z tych parametrów skonfigurowane przy użyciu szablonu administracyjnego różnią się od wartości skonfigurowanych w graficznym interfejsie użytkownika, wartości z szablonu mają pierwszeństwo i są uwzględniane od razu, a parametry przedstawione w graficznym interfejsie użytkownika są odpowiednio zmieniane.

W poniższych podtematach opisano poszczególne sposoby konfiguracji oraz parametry, które można za ich pomocą ustawić.

7.2.1 Parametry konfigurowane przy użyciu szablonu administracyjnego

Poniżej podano parametry komponentów programu Acronis Backup & Recovery 10, które można skonfigurować przy użyciu szablonu administracyjnego Acronis Administrative Template. Aby uzyskać informacje o sposobie stosowania szablonu administracyjnego, zobacz Jak stosować szablon Acronis Administrative Template (s. 378).

Szablon administracyjny zawiera parametry konfiguracyjne agenta programu Acronis Backup & Recovery 10, serwera zarządzania Acronis Backup & Recovery 10 Management Server i węzła magazynowania Acronis Backup & Recovery 10 Storage Node, które opisano w odpowiednich podtematach niniejszego tematu.

Jak załadować szablon Acronis Administrative Template

Szablon administracyjny Acronis Administrative Template umożliwia precyzyjne konfigurowanie niektórych funkcji związanych z zabezpieczeniami, w tym ustawień zaszyfrowanej komunikacji. Korzystając z mechanizmu zasad grupy firmy Microsoft, ustawienia zasad szablonu można zastosować do pojedynczego komputera, jak również do całej domeny.

Aby załadować szablon Acronis Administrative Template

1. Uruchom Edytor obiektów zasad grupy w systemie Windows (%windir%\system32\gpedit.msc).
2. Otwórz obiekt zasad grupy (GPO), który chcesz edytować.
3. Rozwiń węzeł **Konfiguracja komputera**.
4. Kliknij prawym przyciskiem myszy **Szablony administracyjne**.
5. Kliknij **Dodaj/Usuń szablony**.
6. Kliknij **Dodaj**.
7. Przejdź do szablonu Acronis Administrative Template (\Program Files\Common Files\Acronis\Agent \Acronis_agent.adm lub \Program Files\Acronis\BackupAndRecoveryConsole\Acronis_agent.adm) i kliknij **Otwórz**.

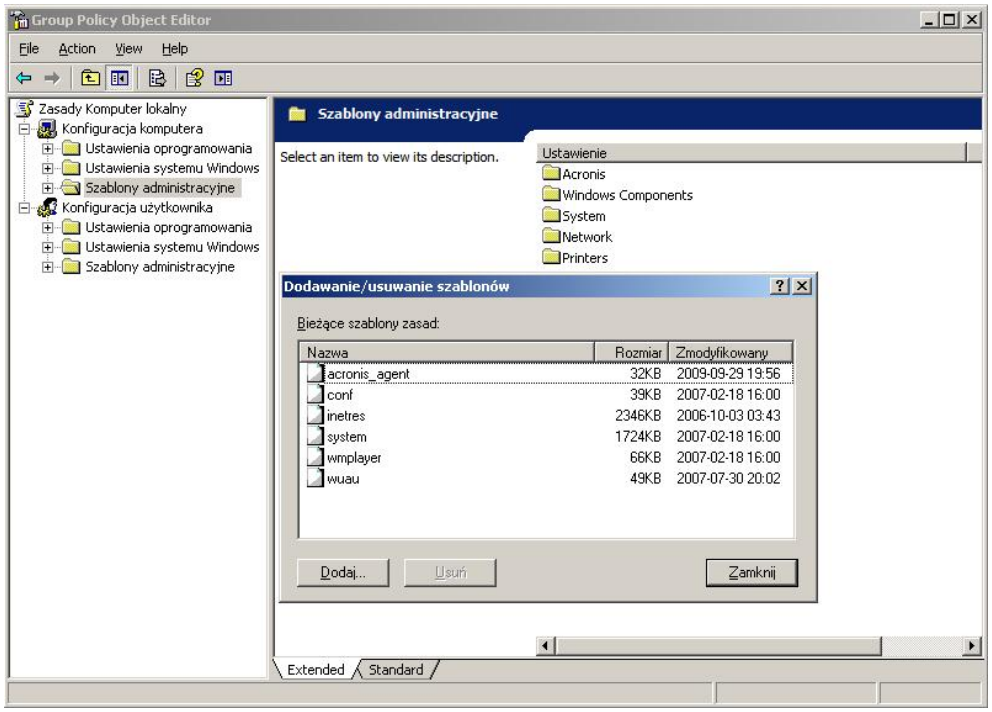
Załadowany szablon można otworzyć i zmodyfikować żądane ustawienia. Po załadowaniu szablonu lub zmodyfikowaniu jego ustawień należy ponownie uruchomić skonfigurowane komponenty lub niektóre z ich usług.

Szczegółowe informacje na temat edytora obiektów zasad grupy w systemie Windows są dostępne pod adresem:

http://msdn2.microsoft.com/pl-pl/library/aa374163.aspx

Szczegółowe informacje na temat zasad grup są dostępne pod adresem:

http://msdn2.microsoft.com/pl-pl/library/aa374177.aspx



Acronis Backup & Recovery 10 Storage Node

Poniżej podano parametry węzła magazynowania Acronis Backup & Recovery 10 Storage Node, które można skonfigurować przy użyciu szablonu administracyjnego Acronis Administrative Template.

Client Connection Limit

Opis: określa maksymalną liczbę równoczesnych połączeń z węzłem magazynowania ze strony agentów tworzących kopie zapasowe lub odzyskujących dane.

Możliwe wartości: Dowolna liczba całkowita z zakresu od **1** do **2147483647**

Wartość domyślna: **10**

Agenty programu Acronis Backup & Recovery 10 łączą się z węzłem magazynowania w celu uzyskania dostępu do jego skarbców zarządzanych podczas tworzenia kopii zapasowych lub odzyskiwania. Parametr **Client Connection Limit** określa maksymalną liczbę połączeń, jaką może równocześnie obsłużyć węzeł magazynowania.

Po osiągnięciu tego ograniczenia wobec agentów oczekujących na połączenie węzeł magazynowania zastosuje kolejkę kopii zapasowych (zobacz następny parametr).

Backup Queue Limit

Opis: określa maksymalną liczbę komponentów programu Acronis Backup & Recovery 10 w kolejce kopii zapasowych węzła magazynowania.

Możliwe wartości: Dowolna liczba całkowita z zakresu od **1** do **2147483647**

Wartość domyślna: **50**

Kolejka kopii zapasowych to lista komponentów programu Acronis Backup & Recovery 10 oczekujących na połączenie z węzłem magazynowania lub aktualnie z nim połączonych (zobacz poprzedni parametr).

Jeśli liczba komponentów w kolejce kopii zapasowych będzie równa wartości ustawienia **Backup Queue Limit**, węzeł magazynowania nie umieści w kolejce kolejnego komponentu próbującego nawiązać połączenie.

W takim przypadku próba połączenia się komponentu z węzłem magazynowania zakończy się niepowodzeniem. Jeśli komponentem będzie agent programu Acronis Backup & Recovery 10, odpowiednie zadanie tworzenia kopii zapasowej lub odzyskiwania zostanie zatrzymane ze statusem **Zakończone niepowodzeniem**.

Vault Warnings and Limits

Określa ilość wolnego miejsca w skarbcu (zarówno bezwzględnie, jak i procentowo), poniżej której w dzienniku rejestrowane jest ostrzeżenie lub błąd.

Ten parametr ma następujące ustawienia:

Vault Free Space Warning Limit

Opis: określa ilość wolnego miejsca w skarbcu zarządzanym (w megabajtach), poniżej której rejestrowane jest ostrzeżenie w dzienniku węzła magazynowania.

Możliwe wartości: Dowolna liczba całkowita z zakresu od **0** do **2147483647**

Wartość domyślna: **200**

Wolne miejsce w skarbcu to ilość wolnego miejsca na nośniku, takim jak wolumin dysku, na którym znajduje się skarbiec.

Jeśli ilość wolnego miejsca w skarbcu jest równa lub mniejsza od wartości ustawienia **Vault Free Space Warning Limit**, w dzienniku węzła magazynowania rejestrowane jest ostrzeżenie wskazujące ten skarbiec. Ostrzeżenia węzła magazynowania można wyświetlić na pulpicie nawigacyjnym.

Vault Free Space Warning Percentage

Opis: określa ilość wolnego miejsca w skarbcu zarządzanym (wyrażoną jako procent jego całkowitego rozmiaru), poniżej której rejestrowane jest ostrzeżenie w dzienniku węzła magazynowania.

Możliwe wartości: Dowolna liczba całkowita z zakresu od **0** do **100**

Wartość domyślna: **10**

Całkowity rozmiar skarbca to suma wolnego miejsca w skarbcu oraz rozmiaru wszystkich archiwów znajdujących się w tym skarbcu.

Na przykład przyjmijmy, że na woluminie dysku znajdują się dwa skarbce: skarbiec A i skarbiec B. Przyjmijmy ponadto, że rozmiar archiwów w skarbcu A wynosi 20 GB, a rozmiar archiwów w skarbcu B — 45 GB.

Jeśli na woluminie jest 5 GB wolnego miejsca, całkowity rozmiar skarbca A wynosi 20 GB + 5 GB = 25 GB, a skarbca B — 45 GB + 5 GB = 50 GB, niezależnie od rozmiaru woluminu.

Procent wolnego miejsca w skarbcu to iloraz ilości wolnego miejsca w skarbcu i całkowitego rozmiaru skarbca. W poprzednim przykładzie w skarbcu A jest 5 GB / 25 GB = 20% wolnego miejsca, a w skarbcu B — 5 GB / 50 GB = 10% wolnego miejsca.

Jeśli procent wolnego miejsca w skarbcu jest równy lub mniejszy od wartości ustawienia **Vault Free Space Warning Percentage**, w dzienniku węzła magazynowania rejestrowane jest ostrzeżenie wskazujące ten skarbiec. Ostrzeżenia węzła magazynowania można wyświetlić na pulpicie nawigacyjnym.

Uwaga: *Parametry* ***Vault Free Space Warning Limit*** *i* ***Vault Free Space Warning Percentage*** *są niezależne od siebie. Ostrzeżenie jest rejestrowane po każdym przekroczeniu dowolnej z tych wartości progowych.*

Vault Free Space Error Limit

Opis: określa ilość wolnego miejsca w skarbcu zarządzanym (w megabajtach), poniżej której rejestrowany jest błąd w dzienniku węzła magazynowania, a skarbiec zamykany jest dla wszelkich kopii zapasowych.

Możliwe wartości: Dowolna liczba całkowita z zakresu od **0** do **2147483647**

Wartość domyślna: **50**

Jeśli ilość wolnego miejsca w skarbcu jest równa lub mniejsza od wartości ustawienia **Vault Free Space Error Limit**, w dzienniku węzła magazynowania rejestrowany jest błąd. Tworzenie kopii zapasowych w skarbcu będzie kończyć się niepowodzeniem aż do momentu, gdy ilość wolnego miejsca znajdzie się powyżej limitu.

Vault Database Free Space Warning Limit

Opis: określa ilość wolnego miejsca (w megabajtach) na woluminie zawierającym bazę danych skarbca zarządzanego, poniżej której rejestrowane jest ostrzeżenie w dzienniku węzła magazynowania.

Możliwe wartości: Dowolna liczba całkowita z zakresu od **0** do **2147483647**

Wartość domyślna: **20**

Jeśli ilość wolnego miejsca na woluminie zawierającym bazę danych skarbca zarządzanego jest mniejsza niż wartość ustawienia **Vault Database Free Space Warning Limit**, w dzienniku węzła magazynowania rejestrowane jest ostrzeżenie wskazujące ten skarbiec. Ostrzeżenia węzła magazynowania można wyświetlić na pulpicie nawigacyjnym.

Baza danych jest przechowywana w węźle magazynowania w folderze lokalnym, którego nazwa została określona w ustawieniu **Ścieżka bazy danych** podczas tworzenia skarbca.

Vault Database FreeSpace Error Limit

Opis: określa ilość wolnego miejsca (w megabajtach) na woluminie zawierającym bazę danych skarbca zarządzanego, poniżej której rejestrowany jest błąd w dzienniku węzła magazynowania, a skarbiec zamykany jest dla wszelkich kopii zapasowych.

Możliwe wartości: Dowolna liczba całkowita z zakresu od **0** do **2147483647**

Wartość domyślna: **10**

Jeśli ilość wolnego miejsca na dysku zawierającym bazę danych skarbca zarządzanego jest mniejsza niż wartość ustawienia **Vault Database Free Space Error Limit**, w dzienniku węzła magazynowania rejestrowany jest błąd. Tworzenie kopii zapasowych w skarbcu będzie kończyć się niepowodzeniem aż do momentu, gdy ilość wolnego miejsca znajdzie się powyżej limitu.

Błędy węzła magazynowania można wyświetlić na pulpicie nawigacyjnym.

Baza danych jest przechowywana w węźle magazynowania w folderze lokalnym, którego nazwa została określona w ustawieniu **Ścieżka bazy danych** podczas tworzenia skarbca.

Acronis Backup & Recovery 10 Management Server

Poniżej znajdują się parametry serwera Acronis Backup & Recovery 10, które można ustawić za pomocą szablonu Acronis Administrative Template.

Collecting Logs

Określa, kiedy jest wykonywane zbieranie dzienników z komputerów zarządzanych przez serwer Acronis Backup & Recovery 10 Management Server.

Parametr ten przyjmuje dwa ustawienia:

Trace State

Opis: Określa, czy z komputerów zarejestrowanych mają być zbierane wpisy dzienników na temat zdarzeń dotyczących komponentów.

Możliwe wartości: **Prawda** lub **Fałsz**

Wartość domyślna: Prawda

Trace Level

Opis: Określa minimalny poziom ważności zbieranych wpisów. Zbierane będą wyłącznie wpisy o poziomie ważności określonym w ustawieniu **Trace Level** lub wyższym.

Możliwe wartości: **0** (zdarzenie wewnętrzne), **1** (informacje dotyczące debugowania), **2** (informacje), **3** (ostrzeżenie), **4** (błąd), **5** (błąd krytyczny)

Wartość domyślna: 0 (zbierane będą wszystkie wpisy)

Log Cleanup Rules

Określa sposób czyszczenia centralnego dziennika zdarzeń przechowywanego w bazie danych raportowania serwera zarządzania.

Ten parametr ma następujące ustawienia:

Max Size

Opis: Określa maksymalny (w kilobajtach) rozmiar centralnego dziennika zdarzeń.

Możliwe wartości: Dowolna liczba całkowita z zakresu od **0** do **2147483647**

Wartość domyślna: **1048576** (1 GB)

Percentage to Keep

Opis: Określa procentowo maksymalny rozmiar dziennika, który ma być zachowany podczas czyszczenia.

Możliwe wartości: Dowolna liczba całkowita z zakresu od **0** do **100**

Wartość domyślna: **95**

Aby zapoznać się ze szczegółami dotyczącymi czyszczenia centralnego dziennika zdarzeń, zobacz Reguły czyszczenia dziennika (s. 101).

Windows Event Log

Określa, kiedy zdarzenia serwera zarządzania Acronis Backup & Recovery 10 mają być zapisywane w dzienniku zdarzeń Aplikacje systemu Windows.

Parametr ten przyjmuje dwa ustawienia:

Trace State

Opis: Określa, czy zdarzenia dotyczące serwera Acronis Backup & Recovery 10 Management Server mają być rejestrowane w dzienniku zdarzeń.

Możliwe wartości: **Prawda** lub **Fałsz**

Wartość domyślna: Fałsz

Trace Level

Opis: Określa minimalny poziom ważności zdarzeń rejestrowanych w dzienniku zdarzeń. Rejestrowane będą wyłącznie zdarzenia o poziomie ważności określonym w ustawieniu **Trace Level** lub wyższym.

Możliwe wartości: **0** (zdarzenie wewnętrzne), **1** (informacje dotyczące debugowania), **2** (informacje), **3** (ostrzeżenie), **4** (błąd), **5** (błąd krytyczny)

Wartość domyślna: **4** (jeśli ustawienie **Trace State** [Stan śledzenia] ma wartość **True** [Prawda], będą rejestrowane tylko błędy i błędy krytyczne)

SNMP

Określa typy zdarzeń serwera zarządzania, które będą wysyłały powiadomienia za pomocą protokołu SNMP.

Ten parametr ma następujące ustawienia:

Trace State

Opis: Określa, czy mają być wysyłane powiadomienia SNMP.

Możliwe wartości: **Prawda** lub **Fałsz**

Wartość domyślna: Fałsz

Trace Level

Opis: Określa minimalny poziom ważności zdarzeń, o których mają być wysyłane powiadomienia SNMP. Wysyłane będą wyłącznie powiadomienia dotyczące zdarzeń o poziomie ważności określonym w ustawieniu **Trace Level** lub wyższym.

Możliwe wartości: **0** (zdarzenie wewnętrzne), **1** (informacje dotyczące debugowania), **2** (informacje), **3** (ostrzeżenie), **4** (błąd), **5** (błąd krytyczny)

Wartość domyślna: 4 (będą wysyłane tylko błędy i błędy krytyczne — jeśli ustawienie **Trace State** ma wartość **True**)

SNMP Address

Opis: Określa nazwę sieciową lub adres IP serwera SNMP.

Możliwe wartości: Dowolny ciąg znaków o długości od 0 do 32765 znaków

Wartość domyślna: Pusty ciąg

SNMP Community

Opis: Określa nazwę społeczności do powiadomień SNMP.

Możliwe wartości: Dowolny ciąg znaków o długości od 0 do 32765 znaków

Wartość domyślna: public

Synchronizacja

Określa sposób łączenia się serwera Acronis Backup & Recovery 10 Management Server z komputerami zarejestrowanymi w celu wdrażania scentralizowanych zasad, pobierania dzienników i informacji o stanie planów tworzenia kopii zapasowych oraz wykonywania podobnych czynności — ogólnie nazywanych synchronizacją.

Ten parametr ma następujące ustawienia:

Maximum Connections

Opis: Określa maksymalną liczbę równoczesnych aktywnych połączeń synchronizacji.

Możliwe wartości: Dowolna liczba całkowita z zakresu od 1 do 500

Wartość domyślna: 200

Jeśli łączna liczba komputerów zarejestrowanych online nie przekracza wartości **Maximum Connections**, połączenia z tymi komputerami są zawsze aktywne, a serwer zarządzania regularnie przeprowadza synchronizację z każdym komputerem.

W przeciwnym przypadku liczba zarejestrowanych komputerów zależy od przydzielonej liczby jednoczesnych połączeń. Po wykonaniu synchronizacji komputera, serwer zarządzania może odłączyć się od niego i wykorzystać nieużywane połączenie do synchronizacji innego komputera itd.

(Uwaga: Połączenia z komputerami o wysokim priorytecie synchronizacji — zobacz **Period-High Priority** w dalszej części tego tematu — zazwyczaj są stale aktywne).

Połączenia synchronizacyjne są niezależne od połączeń między programami, np. między serwerem Acronis Backup & Recovery 10 Management Server i konsolą Acronis Backup & Recovery 10 Management Console.

Maximum Workers

Opis: Określa maksymalną liczbę wątków synchronizacji.

Możliwe wartości: Dowolna liczba całkowita z zakresu od 1 do 100

Wartość domyślna: 30

W celu synchronizacji zarejestrowanego komputera, z którym zostało już nawiązane połączenie, serwer zarządzania wykorzystuje specjalne wątki nazywane wątkami roboczymi.

Każdy wątek roboczy wykonuje w danym momencie synchronizację dokładnie jednego komputera.

Podłączony komputer do synchronizacji oczekuje na dostępność wątku roboczego. Z tego względu rzeczywista liczba wątków roboczych nigdy nie przekracza maksymalnej liczby połączeń (zobacz ustawienie **Maximum Connections** opisane powyżej).

Period (w sekundach)

Opis: Określa (w sekundach) częstotliwość wykonywania synchronizacji na komputerach o normalnym priorytecie synchronizacji — zwykle są to komputery, na których aktualnie nie są uruchomione scentralizowane zadania tworzenia kopii zapasowych.

Możliwe wartości: Dowolna liczba całkowita z zakresu od 120 do 2147483647

Wartość domyślna: 120

Serwer Acronis Backup & Recovery 10 Management Server próbuje wykonać jedną synchronizację każdego komputera o normalnym priorytecie w czasie określonym (w sekundach) w ustawieniu **Period**, korzystając w tym celu z dostępnego wątku roboczego (zobacz ustawienie **Maximum Workers** opisane powyżej).

Jeśli liczba wątków roboczych jest niższa od komputerów o standardowym priorytecie, rzeczywisty odstęp między synchronizacjami może być dłuższy od wartości danego parametru.

Period-High Priority (sekund)

Opis: Określa (w sekundach) częstotliwość wykonywania synchronizacji na komputerach o wysokim priorytecie synchronizacji — zwykle są to komputery, na których aktualnie są uruchomione scentralizowane zadania tworzenia kopii zapasowych.

Możliwe wartości: Dowolna liczba całkowita z zakresu od 15 do 2147483647

Wartość domyślna: 15

Jest to parametr analogiczny do parametru **Period** opisanego powyżej.

Real-Time Monitoring

Opis: Określa, czy komputery zarejestrowane należy monitorować w czasie rzeczywistym, zamiast stosować mechanizm sondowania.

Możliwe wartości: **Prawda** lub **Fałsz**

Wartość domyślna: Fałsz

W domyślnej konfiguracji serwer Acronis Backup & Recovery 10 łączy się z zarejestrowanymi komputerami w celu wykonania synchronizacji danych; w szczególności, w celu pobrania np. dzienników kopii zapasowych. Jest to znane jako mechanizm odpytywania.

Jeśli ustawienie **Real Time Monitoring** ma wartość **True**, zawsze po pojawieniu się nowych danych serwer zarządzania wysyła do komputerów żądanie udostępnienia tych danych, a następnie przechodzi do trybu nasłuchiwania. Jest to znane jako bieżący monitoring.

Pozwala on na zmniejszenie ilości danych przesyłanych przez sieć, np. gdy scentralizowane zadania tworzenia kopii zapasowych są wykonywane rzadko. Jednak ustawienie to działa skutecznie tylko wtedy, gdy liczba zarejestrowanych komputerów jest ograniczona.

Monitorowania w czasie rzeczywistym nie należy włączać, gdy liczba komputerów zarejestrowanych przekracza maksymalną liczbę równoczesnych połączeń (zobacz **Maximum Connections** we wcześniejszej części tego tematu).

Second Connection Attempt

Opis: Określa, czy należy wykonać próbę połączenia się z komputerem zarejestrowanym przy użyciu jego ostatniego znanego adresu IP, jeśli próba połączenia z tym komputerem przy użyciu nazwy hosta zakończyła się niepowodzeniem.

Możliwe wartości: **Prawda** lub **Fałsz**

Wartość domyślna: Fałsz

Podczas próby połączenia z zarejestrowanym komputerem, serwer Acronis Backup & Recovery 10 Management Server próbuje najpierw użyć nazwy sieciowej komputera, jeśli została wprowadzona.

Jeśli ustawienie **Second Connection Attempt** ma wartość **True** i połączenie z komputerem przy użyciu jego nazwy sieciowej zakończyło się niepowodzeniem, serwer zarządzania spróbuje połączyć się z tym komputerem przy użyciu ostatniego adresu IP skojarzonego z jego nazwą sieciową.

Określenie wartości **True** w ustawieniu Second ConnectionAttempt jest zalecane tylko w sieciach, w których często występują problemy z serwerami DNS, a adresy IP komputerów zmieniają się rzadko, tak jak w przypadku stałych adresów IP lub długich czasów dzierżawy DHCP.

Ustawienie to nie odnosi się do komputerów, które zostały dodane do serwera zarządzania za pomocą adresu IP.

Próg w trakcie trybu offline (w sekundach)

Opis: Określa maksymalny odstęp (w sekundach) między kolejnymi próbami połączenia się z komputerem zarejestrowanym, który wydaje się znajdować w trybie offline.

Możliwe wartości: Dowolna liczba całkowita z zakresu od 120 do 2147483647

Wartość domyślna: 1800

Zwykle serwer zarządzania łączy się z każdym komputerem zarejestrowanym co pewien czas (zobacz ustawienia **Period** i **Period-High Priority** we wcześniejszych częściach tej sekcji). Jeśli serwer zarządzania wykryje, że komputer jest w trybie offline, czas ten zostanie podwojony i będzie podwajany przy każdej kolejnej próbie aż do osiągnięcia wartości określonej w ustawieniu **Offline Period Threshold**. Gdy komputer wróci do trybu online, odstęp czasu zostanie przywrócony do normalnego.

Pozwala to zwiększyć wydajność wykorzystania zasobów serwera zarządzania i zmniejszyć obciążenie sieci.

Backup

Określa lokalizację i początkowy rozmiar magazynu migawki — pliku tymczasowego używanego podczas tworzenia kopii zapasowej danych za pomocą migawki. Plik ten jest usuwany zaraz po zakończeniu tworzenia kopii zapasowej.

Przy domyślnych ustawieniach magazyn migawki jest tworzony w folderze plików tymczasowych systemu Windows i zajmuje 50 procent miejsca dostępnego na woluminie zawierającym dany folder. Rozmiar ten może wzrosnąć, jeśli migawka wymaga więcej miejsca.

Warto rozważyć zwiększenie początkowego rozmiaru magazynu migawki lub umieszczenie go na innym woluminie, jeśli występują problemy podczas tworzenia kopii zapasowej danych, które często ulegają zmianie podczas tworzenia kopii.

Parametr ten jest używany podczas tworzenia zasad tworzenia kopii zapasowych i ma zastosowanie do wszystkich scentralizowanych planów tworzenia kopii zapasowych, które powstaną na podstawie tych zasad. Zmiany tego parametru nie wpływają na już istniejące zasady tworzenia kopii zapasowych (i ich scentralizowane plany).

Ten parametr ma następujące ustawienia:

Snapshot Storage Path

Opis: Określa folder, w którym zostanie umieszczony magazyn migawki.

Możliwe wartości: Dowolny ciąg znaków o długości od 0 do 32765 znaków

Wartość domyślna: Pusty ciąg

Pusty ciąg oznacza folder na pliki tymczasowe określany przeważnie przez zmienną środowiskową TMP lub TEMP.

Można określić lokalny folder na dowolnym woluminie, także tym, dla którego jest wykonywana kopia zapasowa.

Snapshot Storage Absolute Size

Opis: Określa w megabajtach początkowy rozmiar magazynu migawki.

Możliwe wartości: Dowolna liczba całkowita z zakresu od **0** do **2147483647**

Wartość domyślna: **0**

Wartość **0** oznacza, że serwer zarządzania użyje ustawienia **Snapshot Storage Relative Size**.

Rozmiar początkowy nie może być większy niż ilość dostępnego miejsca minus 50 MB.

Snapshot Storage Relative Size

Ustawienie to jest efektywne tylko wtedy, gdy ustawienie **Snapshot Storage Absolute Size** wynosi **0**.

Opis: Określa początkowy rozmiar magazynu migawki jako procent miejsca dostępnego na dysku podczas uruchamiania procesu tworzenia kopii zapasowej.

Możliwe wartości: Dowolna liczba całkowita z zakresu od **0** do **100**

Wartość domyślna: **50**

Wartość **0** oznacza, że magazyn migawki nie zostanie utworzony.

Rozmiar początkowy nie może być większy niż ilość dostępnego miejsca minus 50 MB.

Migawki można wykonywać nawet bez magazynu.

Rozmiar magazynu migawki nie wpływa na rozmiar kopii zapasowej.

Acronis Backup & Recovery 10 Agent dla systemu Windows

Poniżej znajdują się parametry agenta Acronis Backup & Recovery 10, które można ustawić za pomocą szablonu Acronis Administrative Template.

Licencjonowanie

Określa, jak często agent kontroluje licencję na serwerze licencji i ile czasu może pracować bez serwera licencji.

License Check Interval (w dniach)

Opis: Określa (w dniach) częstotliwość sprawdzania dostępności licencji na serwerze Acronis License Server.

Możliwe wartości: Dowolna liczba całkowita z zakresu od **0** do **5**

Wartość domyślna: 1

Agent Acronis Backup & Recovery 10 kontroluje regularnie, czy na serwerze licencji znajduje się klucz licencji. Pierwsze sprawdzenie odbywa się przy każdym uruchomieniu agenta programu Acronis Backup & Recovery 10, a następnie obecność licencji sprawdzana jest z częstotliwością określoną w dniach w ustawieniu **License Check Interval**.

Gdy agent nie może się połączyć z serwerem licencji, w dzienniku agenta umieszczane jest ostrzeżenie. Można je wyświetlić na pulpicie nawigacyjnym..

Jeśli ustawienie ma wartość **0**, obecność licencji nie będzie sprawdzana. Brak licencji spowoduje, że program Acronis Backup & Recovery 10 przestanie działać po upływie liczby dni określonej w ustawieniu **Maximum Time Without License Server** (zobacz następny parametr).

Zobacz także ustawienie **License Server Connection Retry Interval** w dalszej części tego tematu.

Maximum Time Without License Server (w dniach)

Opis: Określa czas (w dniach), po upływie którego program Acronis Backup & Recovery 10 przestanie działać.

Możliwe wartości: Dowolna liczba całkowita z zakresu od **0** do **60**

Wartość domyślna: 30

Jeśli serwer licencji Acronis License Server będzie niedostępny, program Acronis Backup & Recovery 10 będzie działać w pełni funkcjonalnie przez liczbę dni określoną w ustawieniu **Maximum Time Without License Server**. Czas ten jest liczony od chwili instalacji lub ostatniego pomyślnego sprawdzenia licencji.

License Server Connection Retry Interval (w godzinach)

Opis: Określa odstęp (w godzinach) między próbami połączenia, gdy serwer licencji Acronis License Server jest niedostępny.

Możliwe wartości: Dowolna liczba całkowita z zakresu od **0** do **24**

Wartość domyślna: 1

Jeśli podczas sprawdzania dostępności klucza licencyjnego (zobacz ustawienie **License Check Interval** we wcześniejszej części tego tematu) agent programu Acronis Backup

& Recovery 10 nie będzie mógł połączyć się z serwerem licencji, ponowi próbę połączenia po upływie liczby godzin określonej w ustawieniu **License Server Connection Retry Interval**.

Jeśli ustawienie ma wartość **0**, próby ponownego połączenia nie będą podejmowane. Agent sprawdzi dostępność licencji po upływie czasu, który określono w ustawieniu **License Check Interval**.

License Server Address

Opis: Określa nazwę sieciową lub adres IP serwera Acronis License Server.

Możliwe wartości: Dowolny ciąg znaków o długości od 0 do 32765 znaków

Wartość domyślna: Pusty ciąg

Log Cleanup Rules

Określa sposób czyszczenia dziennika agenta.

Ten parametr ma następujące ustawienia:

Max Size

Opis: Określa maksymalny (w kilobajtach) rozmiar folderu z dziennikiem agenta.

Możliwe wartości: Dowolna liczba całkowita z zakresu od **0** do **2147483647**

Wartość domyślna: **1048576** (1 GB)

Percentage To Keep

Opis: Określa procentowo maksymalny rozmiar dziennika, który ma być zachowany podczas czyszczenia.

Możliwe wartości: Dowolna liczba całkowita z zakresu od **0** do **100**

Wartość domyślna: **95**

Aby zapoznać się ze szczegółami dotyczącymi czyszczenia dziennika agenta, zobacz Reguły czyszczenia dziennika (s. 108).

Windows Event Log

Określa, kiedy zdarzenia agenta Acronis Backup & Recovery 10 mają być zapisywane w dzienniku zdarzeń Aplikacje systemu Windows.

Parametr ten przyjmuje dwa ustawienia:

Trace State

Opis: Określa, czy zdarzenia dotyczące agenta mają być rejestrowane w dzienniku zdarzeń.

Możliwe wartości: **Prawda** lub **Fałsz**

Wartość domyślna: Fałsz

Trace Level

Opis: Określa minimalny poziom ważności zdarzeń rejestrowanych w dzienniku zdarzeń. Rejestrowane będą wyłącznie zdarzenia o poziomie ważności określonym w ustawieniu **Trace Level** lub wyższym.

Możliwe wartości: **0** (zdarzenie wewnętrzne), **1** (informacje dotyczące debugowania), **2** (informacje), **3** (ostrzeżenie), **4** (błąd), **5** (błąd krytyczny)

Wartość domyślna: **4** (jeśli ustawienie **Trace State** [Stan śledzenia] ma wartość **True** [Prawda], będą rejestrowane tylko błędy i błędy krytyczne)

SNMP

Określa typy zdarzeń agenta, które będą wysyłały powiadomienia za pomocą protokołu SNMP.

Ten parametr ma następujące ustawienia:

Trace State

Opis: Określa, czy mają być wysyłane powiadomienia SNMP.

Możliwe wartości: **Prawda** lub **Fałsz**

Wartość domyślna: Fałsz

Trace Level

Opis: Określa minimalny poziom ważności zdarzeń, o których mają być wysyłane powiadomienia SNMP. Wysyłane będą wyłącznie powiadomienia dotyczące zdarzeń o poziomie ważności określonym w ustawieniu **Trace Level** lub wyższym.

Możliwe wartości: **0** (zdarzenie wewnętrzne), **1** (informacje dotyczące debugowania), **2** (informacje), **3** (ostrzeżenie), **4** (błąd), **5** (błąd krytyczny)

Wartość domyślna: **4** (jeśli ustawienie **Trace State** [Stan śledzenia] ma wartość **True** [Prawda], będą rejestrowane tylko błędy i błędy krytyczne)

SNMP Address

Opis: Określa nazwę sieciową lub adres IP serwera SNMP.

Możliwe wartości: Dowolny ciąg znaków o długości od 0 do 32765 znaków

Wartość domyślna: Pusty ciąg

SNMP Community

Opis: Określa nazwę społeczności do powiadomień SNMP.

Możliwe wartości: Dowolny ciąg znaków o długości od 0 do 32765 znaków

Wartość domyślna: public

Backup

Określa lokalizację i początkowy rozmiar magazynu migawki — pliku tymczasowego używanego podczas tworzenia kopii zapasowej danych za pomocą migawki. Plik ten jest usuwany zaraz po zakończeniu tworzenia kopii zapasowej.

Przy domyślnych ustawieniach magazyn migawki jest tworzony w folderze plików tymczasowych systemu Windows i początkowo zajmuje 50 procent miejsca dostępnego na woluminie zawierającym dany folder. Rozmiar ten może wzrosnąć, jeśli migawka wymaga więcej miejsca.

Warto rozważyć zwiększenie początkowego rozmiaru magazynu migawki lub umieszczenie go na innym woluminie, jeśli występują problemy podczas tworzenia kopii zapasowej danych, które często ulegają zmianie podczas tworzenia kopii.

Parametr używany podczas tworzenia planu tworzenia kopii zapasowych. Zmiana tego parametru nie wpływa na istniejące plany tworzenia kopii zapasowych.

Ten parametr ma następujące ustawienia:

Snapshot Storage Path

Opis: Określa folder, w którym zostanie utworzony magazyn migawki.

Możliwe wartości: Dowolny ciąg znaków o długości od 0 do 32765 znaków

Wartość domyślna: Pusty ciąg

Pusty ciąg oznacza folder na pliki tymczasowe określany przeważnie przez zmienną środowiskową TMP lub TEMP.

Można określić lokalny folder na dowolnym woluminie, także tym, dla którego jest wykonywana kopia zapasowa.

Snapshot Storage Absolute Size

Opis: Określa w megabajtach początkowy rozmiar magazynu migawki.

Możliwe wartości: Dowolna liczba całkowita z zakresu od **0** do **2147483647**

Wartość domyślna: **0**

Wartość **0** oznacza, że serwer zarządzania użyje ustawienia **Snapshot Storage Relative Size**.

Rozmiar początkowy nie może być większy niż ilość dostępnego miejsca minus 50 MB.

Snapshot Storage Relative Size

Ustawienie to jest efektywne tylko wtedy, gdy ustawienie **Snapshot Storage Absolute Size** wynosi **0**.

Opis: Określa początkowy rozmiar magazynu migawki jako procent miejsca dostępnego na dysku podczas uruchamiania procesu tworzenia kopii zapasowej.

Możliwe wartości: Dowolna liczba całkowita z zakresu od **0** do **100**

Wartość domyślna: **50**

Wartość **0** oznacza, że magazyn migawki nie zostanie utworzony.

Rozmiar początkowy nie może być większy niż ilość dostępnego miejsca minus 50 MB.

Migawki można wykonywać nawet bez magazynu.

Rozmiar magazynu migawki nie wpływa na rozmiar kopii zapasowej.

Acronis Backup & Recovery 10

W tej sekcji przy użyciu szablonu administracyjnego określono parametry połączenia oraz parametry śledzenia zdarzeń dotyczących następujących komponentów programu Acronis Backup & Recovery 10:

- Acronis Backup & Recovery 10 Management Server
- Acronis Backup & Recovery 10 Agent
- Acronis Backup & Recovery 10 Storage Node

Parametry połączenia

Porty zdalnego agenta

Określa port, którego komponent będzie używać do komunikacji przychodzącej i wychodzącej z innymi komponentami Acronis.

Wybierz jedną z następujących opcji:

Nieskonfigurowane

Komponent będzie używać domyślnego numeru portu TCP 9876.

Włączone

Komponent będzie używać określonego portu. Wpisz numer portu w polu **Port TCP serwera**.

Wyłączone

Analogicznie jak **Nieskonfigurowane**.

Opcje szyfrowania klienta

Określa, czy przesyłane dane mają być szyfrowane, gdy komponent służy jako aplikacja kliencka, a także czy należy ufać certyfikatom SSL z podpisem własnym.

Wybierz jedną z następujących opcji:

Nieskonfigurowane

Komponent będzie używać ustawień domyślnych, czyli będzie w miarę możliwości korzystać z szyfrowania oraz ufać certyfikatom SSL z podpisem własnym (zobacz poniższą opcję).

Włączone

Szyfrowanie jest włączone. Wybierz jedno z następujących ustawień opcji **Szyfrowanie**:

Włączone

Przesyłane dane będą szyfrowane, jeśli szyfrowanie zostało włączone w aplikacji serwerowej. W przeciwnym razie dane nie będą szyfrowane.

Wyłączone

Szyfrowanie jest wyłączone. Nie będzie można nawiązać żadnego połączenia z aplikacją serwerową, która wymaga szyfrowania.

Wymagane

Dane będą przesyłane tylko w przypadku, gdy szyfrowanie zostało włączone w aplikacji serwerowej (zobacz sekcję „Opcje szyfrowania serwera"). Przesyłane dane będą szyfrowane.

Parametry uwierzytelniania

Zaznaczenie pola wyboru **Ufaj certyfikatom z podpisem własnym** umożliwia klientowi łączenie się z aplikacjami serwerowymi, które używają certyfikatów SSL z podpisem własnym, takich jak certyfikaty utworzone podczas instalacji komponentów programu Acronis Backup & Recovery 10 (zobacz Certyfikaty SSL (s. 97)).

To pole wyboru powinno być zaznaczone, chyba że w danym środowisku używana jest infrastruktura klucza publicznego (PKI).

Wybierz jedno z następujących ustawień opcji **Użyj uwierzytelniania certyfikatu agenta**:

Nie używaj

Użycie certyfikatów SSL jest wyłączone. Nie będzie można nawiązać żadnych połączeń z aplikacją serwerową, która wymaga użycia certyfikatów SSL.

Użyj, jeśli to możliwe

Użycie certyfikatów SSL jest włączone. Klient będzie używać certyfikatów SSL, jeśli zostały one włączone w aplikacji serwerowej. W przeciwnym razie certyfikaty SSL nie będą używane.

Zawsze używaj

Użycie certyfikatów SSL jest włączone. Połączenie zostanie nawiązane tylko w przypadku, gdy użycie certyfikatów SSL zostało włączone w aplikacji serwerowej.

Wyłączone

Analogicznie jak **Nieskonfigurowane**.

Opcje szyfrowania serwera

Określa, czy przesyłane dane mają być szyfrowane, gdy komponent służy jako aplikacja serwerowa.

Wybierz jedną z następujących opcji:

Nieskonfigurowane

Komponent będzie używać ustawienia domyślnego, czyli będzie w miarę możliwości korzystać z szyfrowania (zobacz poniższą opcję).

Włączone

Szyfrowanie jest włączone. Wybierz jedno z następujących ustawień opcji **Szyfrowanie**:

Włączone

Przesyłane dane będą szyfrowane, jeśli szyfrowanie zostało włączone w aplikacji klienckiej. W przeciwnym razie dane nie będą szyfrowane.

Wyłączone

Szyfrowanie jest wyłączone. Nie będzie można nawiązać żadnego połączenia z aplikacją kliencką, która wymaga szyfrowania.

Wymagane

Dane będą przesyłane tylko w przypadku, gdy szyfrowanie zostało włączone w aplikacji klienckiej (zobacz sekcję „Opcje szyfrowania klienta"). Przesyłane dane będą szyfrowane.

Parametry uwierzytelniania

Wybierz jedno z następujących ustawień opcji **Użyj uwierzytelniania certyfikatu agenta**:

Nie używaj

Użycie certyfikatów SSL jest wyłączone. Nie będzie można nawiązać żadnych połączeń z aplikacją kliencką, która wymaga użycia certyfikatów SSL.

Użyj, jeśli to możliwe

Użycie certyfikatów SSL jest włączone. Serwer będzie używać certyfikatów SSL, jeśli zostały one włączone w aplikacji klienckiej. W przeciwnym razie certyfikaty SSL nie będą używane.

Zawsze używaj

Użycie certyfikatów SSL jest włączone. Połączenie zostanie nawiązane tylko w przypadku, gdy użycie certyfikatów SSL zostało włączone w aplikacji klienckiej.

Wyłączone

Analogicznie jak **Nieskonfigurowane**.

Parametry śledzenia zdarzeń

W systemie Windows zdarzenia występujące w programie Acronis Backup & Recovery 10 można rejestrować w dzienniku zdarzeń, pliku lub w obu miejscach.

Każde zdarzenie ma poziom ważności od zera do pięciu, jak to przedstawiono w następującej tabeli:

Poziom	Nazwa	Opis
0	Nieznany	Zdarzenie, którego poziom ważności jest nieznany lub go nie dotyczy
1	Debugowanie	Zdarzenie służące do celów debugowania
2	Informacja	Zdarzenie informacyjne, takie jak informacja o pomyślnym ukończeniu operacji lub uruchomieniu usługi
3	Ostrzeżenie	Zdarzenie wskazujące na możliwy i nieuchronnie zbliżający się problem, taki jak mało wolnego miejsca w skarbcu
4	Błąd	Zdarzenie występujące w efekcie utraty danych lub zatrzymania działania
5	Krytyczny	Zdarzenie występujące w efekcie zakończenia procesu, takiego jak proces agenta

Parametry śledzenie zdarzeń są określone przez następujące ustawienia w szablonie administracyjnym:

File Trace Minimal Level (Minimalny poziom śledzenia plików)

Opis: Określa minimalny poziom ważności zdarzeń rejestrowanych w pliku. Będą rejestrowane wyłącznie zdarzenia o poziomie ważności równym wartości ustawienia **File Trace Minimal Level** (Minimalny poziom śledzenia plików) lub od niej wyższym.

Możliwe wartości: Dowolny poziom ważności od **nieznanego** do **krytycznego** lub **zablokowany**, aby nie rejestrować żadnych zdarzeń.

Wartość domyślna: 2 (oznacza, że będą rejestrowane zdarzenia o poziomach ważności od 2 do 5)

Pliki dzienników znajdują się w folderze **%ALLUSERSPROFILE%\Application Data\Acronis**, w podfolderze **Logs** konkretnego komponentu.

Win32 Trace Minimal Level (Minimalny poziom śledzenia Win32)

Opis: Określa minimalny poziom ważności zdarzeń rejestrowanych w dzienniku zdarzeń systemowych. Będą rejestrowane wyłącznie zdarzenia o poziomie ważności równym wartości ustawienia **Win32 Trace Minimal Level** (Minimalny poziom śledzenia Win32) lub od niej wyższym.

Możliwe wartości: Dowolny poziom ważności od **nieznanego** do **krytycznego** lub **zablokowany**, aby nie rejestrować żadnych zdarzeń.

Wartość domyślna: 4 (oznacza, że będą rejestrowane zdarzenia dotyczące błędów i błędów krytycznych)

Program jakości obsługi klienta

Określa, czy komputer, na którym jest zainstalowany komponent Acronis Backup & Recovery 10, zostanie objęty Programem jakości obsługi klienta.

Wybierz jedną z następujących opcji:

Nieskonfigurowane

Domyślnie komputer nie jest objęty Programem jakości obsługi klienta.

Włączone

W sekcji **Włącz wysyłanie raportów do firmy Acronis** wybierz jedną z następujących opcji:

Włącz

Informacje na temat konfiguracji sprzętowej, najczęściej i najrzadziej używanych funkcji oraz wszelkich problemów będą automatycznie zbierane z komputera i regularnie wysyłane do firmy Acronis. Wyniki końcowe posłużą do udoskonalenia i zwiększenia funkcjonalności oprogramowania w celu lepszego dostosowania go do potrzeb klientów firmy Acronis. Firma Acronis nie zbiera żadnych danych osobowych. Warunki uczestnictwa można znaleźć w witrynie internetowej firmy Acronis.

Wyłącz

Informacje nie będą wysyłane.

Wyłączone

Analogicznie jak **Nieskonfigurowane**.

7.2.2 Parametry konfigurowane w graficznym interfejsie użytkownika

W graficznym interfejsie użytkownika można skonfigurować następujące parametry:

- dla serwera Acronis Backup & Recovery 10 Management Server: **Zbieranie dzienników**, **Dziennik zdarzeń systemu Windows**, **SNMP**, **Adres SNMP** i **Społeczność SNMP;**
- dla komponentu Acronis Backup & Recovery 10 Agent: **Dziennik zdarzeń systemu Windows**, **SNMP**, **Adres SNMP**, **Społeczność SNMP** i **Program jakości obsługi klienta**.

Opis poszczególnych parametrów można znaleźć w odpowiednim temacie dotyczącym konfiguracji przy użyciu szablonu administracyjnego.

7.2.3 Parametry konfigurowane w rejestrze systemu Windows

Poniżej podano parametry węzła magazynowania Acronis Backup & Recovery 10 Storage Node, które można skonfigurować przez edytowanie rejestru.

Parametry związane z deduplikacją

CompactingTriggerThreshold

Opis: określa w procentach ilość elementów użytych w magazynach danych, poniżej której następuje kompaktowanie.

Możliwe wartości: Dowolna liczba całkowita z zakresu od **0** do **100**

Wartość domyślna: **80**

Klucz rejestru:
HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\ASN\Configuration\StorageNode\CompactingTriggerThreshold

Ponieważ kopie zapasowe są usuwane ze skarbca deduplikacji, magazyny danych deduplikacji (s. 82) mogą zawierać nieużywane elementy: pliki lub bloki dysków, które nie są już związane z żadną kopią zapasową. Węzeł magazynowania przetwarza oba magazyny danych po kolei w celu usunięcia tych elementów. Ta operacja jest nazywana kompaktowaniem.

Ponieważ kompaktowanie wymaga użycia dużej ilości zasobów, powinno się odbywać dopiero po zgromadzeniu odpowiednio dużej ilości nieużywanych elementów.

Parametr **CompactingTriggerThreshold** umożliwia ustawienie zależności pomiędzy dodatkowym miejscem wymaganym do przechowywania nieużywanych elementów a częstotliwością kompaktowania. Im większa wartość tego parametru, tym mniej nieużywanych elementów będzie się znajdowało w magazynach danych, ale kompaktowanie będzie się odbywało częściej.

Ten parametr jest stosowany oddzielnie do kopii zapasowych na poziomie dysków oraz plików. Dlatego kompaktowanie może zostać wykonane dla jednego magazynu danych, a pominięte dla drugiego.

Parametry związane z bazami danych skarbców

Poniższe dwa parametry określają ścieżki do wewnętrznych baz danych węzła magazynowania Acronis Backup & Recovery 10 Storage Node, w których znajdują się informacje o skarbcach zarządzanych.

Baza danych znajdująca się w folderze określonym przez parametr **DatabasePath** jest z reguły mała. Jednak baza danych znajdująca się w folderze określonym przez parametr **TapeDatabasePath** (nazywana bazą danych taśm) może być duża, jeśli biblioteka taśm zawiera tysiące archiwów. W takim przypadku dobrym rozwiązaniem może być zapisanie bazy danych taśm na innym woluminie.

Ważne: *Nie zaleca się modyfikowania poniższych parametrów. Jeśli modyfikacja któregoś z nich jest konieczna, należy ją wykonać przed utworzeniem jakiegokolwiek odpowiadającego mu skarbca zarządzanego (taśm lub innego). W przeciwnym razie węzeł magazynowania utraci dostęp do takich skarbców do czasu ich ponownego dołączenia, a ponowne dołączanie skarbca (szczególnie skarbca deduplikacji) może trwać bardzo długo.*

DatabasePath

Opis: określa folder, w którym węzeł magazynowania Acronis Backup & Recovery 10 Storage Node przechowuje bazę danych skarbców innych niż skarbce taśm.

W tej bazie danych znajduje się lista skarbców zarządzanych przez węzeł magazynowania. Są to skarbce inne niż skarbce taśm (zobacz następny parametr). Zwykle jej rozmiar nie przekracza kilku kilobajtów.

Możliwe wartości: Dowolny ciąg znaków o długości od 0 do 32765 znaków

Wartość domyślna: C:\Program Files\Acronis\StorageNode

Klucz rejestru:
HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\ASN\Configuration\StorageNode\DatabasePath

TapesDatabasePath

Opis: określa folder, w którym węzeł magazynowania Acronis Backup & Recovery 10 Storage Node przechowuje bazę danych skarbców taśm.

W tej bazie danych znajduje się lista skarbców taśm zarządzanych przez węzeł magazynowania. Jej rozmiar zależy od liczby archiwów przechowywanych w bibliotekach taśm i wynosi około 10 MB na każde sto archiwów.

Możliwe wartości: Dowolny ciąg znaków o długości od 0 do 32765 znaków

Wartość domyślna: C:\Documents and Settings\All Users\Application Data\Acronis\BackupAndRecovery\TapeLocation\

Klucz rejestru:
HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\BackupAndRecovery\Configuration\TapeLocation\TapesDatabasePath

7.3 Tworzenie zasad tworzenia kopii zapasowych

Zasady tworzenia kopii zapasowych można zastosować zarówno na komputerach z systemem Windows, jak i z systemem Linux.

Aby utworzyć zasady tworzenia kopii zapasowych, wykonaj poniższe czynności.

Ogólne

Nazwa zasad

[Opcjonalnie] Wprowadź unikatową nazwę zasad tworzenia kopii zapasowych. Dobrze dobrana nazwa umożliwi ich identyfikację pośród innych zasad.

Typ źródła

Wybierz typ elementów do utworzenia kopii zapasowej: **Dysk/woluminy** lub **Pliki**.

Poświadczenia zasad (s. 397)

[Opcjonalnie] W razie potrzeby można zmienić poświadczenia konta zasad. Aby uzyskać dostęp do tej opcji, zaznacz pole wyboru **Widok zaawansowany**.

Komentarze dotyczące zasad

[Opcjonalnie] Wpisz opis zasad tworzenia kopii zapasowych. Aby uzyskać dostęp do tej opcji, zaznacz pole wyboru **Widok zaawansowany**.

Etykieta (s. 222)

[Opcjonalnie] Wpisz etykietę tekstową dla komputerów, których kopie zapasowe chcesz tworzyć. Etykieta umożliwia identyfikację komputera lub grupy komputerów w różnych scenariuszach. Aby uzyskać dostęp do tej opcji, zaznacz pole wyboru **Widok zaawansowany**.

Elementy uwzględniane w kopii zapasowej

Elementy uwzględniane w kopii zapasowej (s. 398)

Określ elementy danych uwzględniane w kopii zapasowej na wszystkich komputerach, na których zostaną wdrożone zasady. Na każdym komputerze agent znajdzie elementy danych przy użyciu określonych reguł. Jeśli na przykład reguła wyboru to [Wszystkie woluminy], zostanie utworzona kopia zapasowa całego komputera.

Poświadczenia dostępu (s. 403)

[Opcjonalnie] Podaj poświadczenia dotyczące danych źródłowych, jeśli konto zasad tworzenia kopii zapasowych nie ma uprawnień dostępu do tych danych. Aby uzyskać dostęp do tej opcji, zaznacz pole wyboru **Widok zaawansowany**.

Wykluczenia (s. 404)

[Opcjonalnie] Skonfiguruj wykluczenia, określając konkretne typy plików, które nie powinny znaleźć się w kopii zapasowej. Aby uzyskać dostęp do tej opcji, zaznacz pole wyboru **Widok zaawansowany**.

Miejsce docelowe kopii zapasowej

Archiwum (s. 405)

Określ ścieżkę do lokalizacji, w której zostanie zapisane archiwum kopii zapasowej, oraz nazwę archiwum. Zaleca się, aby nazwa archiwum była unikatowa w danej lokalizacji. Gdy serwer zarządzania rozpocznie wdrażanie zasad, lokalizacja musi być dostępna.

Poświadczenia dostępu (s. 406)

[Opcjonalnie] Podaj poświadczenia dotyczące lokalizacji, jeśli konto zasad tworzenia kopii zapasowych nie ma uprawnień dostępu do tej lokalizacji. Aby uzyskać dostęp do tej opcji, zaznacz pole wyboru **Widok zaawansowany**.

Komentarze dotyczące archiwum

[Opcjonalnie] Wprowadź komentarze dotyczące archiwum. Aby uzyskać dostęp do tej opcji, zaznacz pole wyboru **Widok zaawansowany**.

Sposób tworzenia kopii zapasowej

Schemat tworzenia kopii zapasowych (s. 407)

Określ czas i częstotliwość tworzenia kopii zapasowych danych, zdefiniuj okres przechowywania utworzonych archiwów kopii zapasowych w wybranej lokalizacji oraz ustal harmonogram dotyczący procedury czyszczenia archiwum. Skorzystaj z dobrze znanych, zoptymalizowanych schematów tworzenia kopii zapasowych, takich jak Dziadek-ojciec-syn i Wieża Hanoi, zdefiniuj schemat niestandardowy lub utwórz kopię zapasową danych jeden raz.

Sprawdzanie poprawności archiwum

Czas sprawdzania poprawności

[Opcjonalnie] Zdefiniuj czas i częstotliwość sprawdzania poprawności oraz czy ma być sprawdzana poprawność całego archiwum, czy ostatniej kopii zapasowej w tym archiwum.

Opcje tworzenia kopii zapasowych

Ustawienia

[Opcjonalnie] Skonfiguruj parametry operacji tworzenia kopii zapasowej, takie jak polecenia poprzedzające/następujące po tworzeniu kopii, maksymalna przepustowość sieci przydzielona do strumienia kopii zapasowej lub stopień kompresji archiwum. Jeśli w tej sekcji nie wykonasz żadnej czynności, zostaną użyte wartości domyślne (s. 109) ustawione na serwerze zarządzania.

Po zmianie dowolnego z ustawień na wartość różną od domyślnej pojawi się nowy wiersz zawierający nowo skonfigurowaną wartość. Stan ustawienia zmieni się z wartości **Domyślne** na **Niestandardowe**. W razie ponownej zmiany ustawienia w wierszu pojawi się nowa wartość, o ile nie będzie to wartość domyślna. W przypadku wartości domyślnej wiersz zniknie. Dlatego w tej sekcji na stronie **Zasady tworzenia kopii zapasowych** wyświetlane są tylko ustawienia różne od domyślnych.

Aby przywrócić wartości domyślne wszystkich ustawień, kliknij **Przywróć domyślne**.

Podczas operacji tworzenia kopii zapasowej domyślne opcje tworzenia kopii zapasowych na zarejestrowanych komputerach są ignorowane.

Konwertuj na maszynę wirtualną

Dotyczy kopii zapasowych **dysku/woluminu**.

Nie dotyczy komputerów z systemem Linux.

Skonfigurowanie regularnej konwersji pozwala uzyskać kopię serwera lub stacji roboczej na maszynie wirtualnej, którą można szybko włączyć w przypadku awarii oryginalnego komputera. Konwersję można wykonać za pomocą dowolnego komputera, który jest zarejestrowany na serwerze zarządzania i zawiera agenta programu Acronis Backup & Recovery 10 o odpowiednich funkcjach. Archiwum należy przechowywać w lokalizacji udostępnionej, takiej jak folder sieciowy lub skarbiec zarządzany. Dzięki temu wybrany komputer będzie miał dostęp do archiwum.

Czas przeprowadzenia konwersji (s. 247)

[Opcjonalnie] Określ, czy należy konwertować każdą pełną, przyrostową lub różnicową kopię zapasową, czy ostatnią utworzoną kopię zapasową według harmonogramu. W razie potrzeby określ harmonogram konwersji.

Host (s. 247)

Określ komputer, który wykona konwersję. Na komputerze musi być zainstalowany Acronis Backup & Recovery 10 Agent dla systemu Windows, Agent dla ESX/ESXi lub Agent dla Hyper-V.

Serwer wirtualizacji (s. 247)

W tym miejscu można wybrać typ i lokalizację wynikowej maszyny wirtualnej. Dostępne opcje zależą od hosta wybranego w poprzednim kroku.

Magazyn (s. 247)

Wybierz magazyn na serwerze wirtualizacji lub folder, w którym zostaną umieszczone pliki maszyny wirtualnej.

Wynikowe maszyny wirtualne

Określ nazwę tworzonych maszyn wirtualnych. Nazwa domyślna składa się ze zmiennych, które odpowiadają nazwie zasad oraz nazwie maszyny, której kopia zapasowa będzie tworzona. Do nazwy można dodać sufiksy, ale nie wolno usuwać zmiennych, ponieważ każda maszyna wirtualna musi mieć własną, unikatową nazwę.

Folder w VMware vCenter

Jeśli serwer zarządzania jest zintegrowany z serwerem vCenter Server, wynikowe maszyny wirtualne pojawią się w folderze **Acronis Backups** w centrum vCenter. Dla maszyn tworzonych w wyniku wykonywania zasad można określić podfolder.

Po wykonaniu wszystkich wymaganych czynności kliknij **OK**, aby utworzyć zasady tworzenia kopii zapasowych.

7.3.1 Poświadczenia zasad

Wprowadź poświadczenia umożliwiające uruchomienie zadań scentralizowanych na komputerach.

Aby określić poświadczenia

1. Wybierz jedną z następujących opcji:
   - **Użyj poświadczeń usługi Acronis**

Zadanie będzie wykonywane z konta usługi Acronis, niezależnie od tego, czy zostanie uruchomione ręcznie czy według harmonogramu.

- **Użyj następujących poświadczeń**

  Zadanie będzie wykonywane z poświadczeniami określonymi przez użytkownika, niezależnie od tego, czy zostanie uruchomione ręcznie czy według harmonogramu.

  Określ:

  - **Nazwa użytkownika**. Wprowadzając nazwę konta użytkownika usługi Active Directory, należy określić również nazwę domeny (DOMENA\Nazwa_użytkownika lub Nazwa_użytkownika@domena).
  - **Hasło**. Hasło dla konta.

2. Kliknij **OK**.

Aby dowiedzieć się więcej na temat poświadczeń usługi Acronis, zobacz sekcję Prawa dotyczące usług Acronis (s. 92).

Aby dowiedzieć się więcej na temat operacji dostępnych w zależności od uprawnień użytkownika, zobacz sekcję Uprawnienia użytkownika na komputerze zarządzanym (s. 34).

7.3.2 Elementy uwzględniane w kopii zapasowej

Określ reguły wyboru dotyczące elementów uwzględnianych w kopii zapasowej, które zostały wybrane w polu **Typ źródła** w sekcji Ogólne.

Reguły wyboru woluminów do kopii zapasowej (s. 398)

Reguły wyboru plików do kopii zapasowej (s. 402)

Reguły wyboru woluminów do kopii zapasowej

Zdefiniuj reguły wyboru woluminów. Na podstawie tych reguł będą tworzone kopie zapasowe woluminów na komputerach, na których zostaną zastosowane zasady.

Aby zdefiniować reguły wyboru woluminów

W pierwszym wierszu wybierz regułę z listy lub wpisz ją ręcznie. Aby dodać kolejną regułę, kliknij kolejny pusty wiersz i wybierz regułę z listy lub wpisz ją ręcznie. Program zapamiętuje reguły wpisane ręcznie, dlatego następnym razem po otwarciu okna reguły te będą dostępne na liście.

W poniższej tabeli znajduje się objaśnienie reguł wstępnie zdefiniowanych, które można wybrać z listy.

Elementy uwzględniane	W kolumnie Woluminy:	Komentarze
Woluminy systemów Windows i Linux		
Wszystkie woluminy	Wpisz lub wybierz: **[Wszystkie woluminy]**	Dotyczy wszystkich woluminów na komputerach z systemem Windows i wszystkich zamontowanych woluminów na komputerach z systemem Linux.
Woluminy systemu Windows		
Wolumin C:	Wpisz **C:** lub wybierz tę pozycję z listy	

Wolumin systemowy	Wpisz lub wybierz: **[SYSTEM]**	Wolumin systemowy zawiera pliki związane ze sprzętem, takie jak Ntldr, Boot.ini i Ntdetect.com, które są potrzebne do uruchomienia systemu Windows. Istnieje tylko jeden wolumin systemowy, nawet jeśli na komputerze jest zainstalowanych wiele systemów operacyjnych Windows. Aby uzyskać więcej informacji, zobacz „Uwaga dotycząca komputerów z systemem Windows” poniżej.
Wolumin startowy	Wpisz lub wybierz: **[BOOT]**	Dotyczy woluminu startowego na komputerze zarejestrowanym. Wolumin startowy zawiera folder systemu operacyjnego Windows i pliki pomocnicze tego systemu (zwykle znajdują się one w folderze Windows\System32). Może on być woluminem systemowym, ale nie musi. Jeśli na komputerze jest zainstalowanych wiele systemów operacyjnych, jest to wolumin startowy systemu operacyjnego, w którym jest zainstalowany agent. Aby uzyskać więcej informacji, zobacz „Uwaga dotycząca komputerów z systemem Windows” poniżej.
Wszystkie woluminy stałe	Wpisz lub wybierz: **[Woluminy stałe]**	Dotyczy wszystkich woluminów innych niż nośniki wymienne. Woluminy stałe obejmują urządzenia SCSI, ATAPI, ATA, SSA, SAS i SATA oraz macierze RAID.
Woluminy systemu Linux		
Pierwsza partycja na pierwszym dysku twardym IDE komputera z systemem Linux	Wpisz lub wybierz: **/dev/hda1**	hda1 to standardowa nazwa urządzenia oznaczająca pierwszą partycję na pierwszym dysku twardym IDE. Aby uzyskać więcej informacji, zobacz „Uwaga dotycząca komputerów z systemem Linux” poniżej.
Pierwsza partycja na pierwszym dysku twardym SCSI komputera z systemem Linux	Wpisz lub wybierz: **/dev/sda1**	sda1 to standardowa nazwa urządzenia oznaczająca pierwszą partycję na pierwszym dysku twardym SCSI. Aby uzyskać więcej informacji, zobacz „Uwaga dotycząca komputerów z systemem Linux” poniżej.
Pierwsza partycja na pierwszym programowym dysku twardym RAID komputera z systemem Linux	Wpisz lub wybierz: **/dev/md1**	md1 to standardowa nazwa urządzenia oznaczająca pierwszą partycję na pierwszym programowym dysku RAID. Aby uzyskać więcej informacji, zobacz „Uwaga dotycząca komputerów z systemem Linux” poniżej.

W nazwach szablonów jest uwzględniana wielkość liter.

Co zawiera kopia zapasowa dysku lub woluminu?

W kopii zapasowej dysku lub woluminu z obsługiwanym systemem plików znajdują się wyłącznie sektory zawierające dane. Zmniejsza to rozmiar wynikowej kopii zapasowej oraz przyspiesza operacje jej tworzenia i odzyskiwania danych.

Windows

Przy tworzeniu kopii zapasowej nie jest uwzględniany plik wymiany (pagefile.sys) ani plik z zawartością pamięci RAM komputera przechodzącego do stanu hibernacji (hiberfil.sys). Po odzyskaniu danych pliki te zostaną ponownie utworzone w odpowiednim miejscu z rozmiarem zerowym.

Kopia zapasowa woluminu zawiera wszystkie pozostałe pliki i foldery wybranego woluminu niezależnie od ich atrybutów (w tym pliki ukryte i systemowe), rekord startowy, tablicę FAT (o ile istnieje), katalog główny i zerową ścieżkę dysku twardego z głównym rekordem rozruchowym MBR. Kod startowy woluminów GPT nie jest uwzględniany przy tworzeniu kopii zapasowej.

Kopia zapasowa dysku zawiera wszystkie woluminy wybranego dysku (w tym woluminy ukryte, takie jak partycje konserwacyjne producenta) oraz ścieżkę zerową głównego rekordu rozruchowego.

Linux

Kopia zapasowa woluminu zawiera wszystkie pliki i foldery wybranego woluminu niezależnie od ich atrybutów, rekord startowy oraz superblok systemu plików.

Kopia zapasowa dysku zawiera wszystkie woluminy dysku oraz ścieżkę zerową i główny rekord rozruchowy.

Kopie zapasowe woluminów z nieobsługiwanymi systemami plików będą tworzone „sektor po sektorze".

Uwaga dotycząca komputerów z systemem Windows

Systemy operacyjne Windows starsze niż Windows 7 i Windows Server 2008 R2 zapisują pliki systemowe i program ładujący na tym samym woluminie, chyba że podczas instalacji został określony inny wolumin. Jeśli pliki systemu Windows i program ładujący znajdują się na tym samym woluminie, wybranie opcji **[SYSTEM]** lub **[BOOT]** wystarcza do utworzenia kopii zapasowej całego systemu operacyjnego. W przeciwnym razie należy wybrać obie opcje: **[SYSTEM]** i **[BOOT]**.

Systemy operacyjne Windows 7, Windows Server 2008 R2 oraz nowsze tworzą specjalny wolumin systemowy o nazwie **System Reserved**. W razie wybrania opcji **[SYSTEM]** program utworzy kopię zapasową tylko tego specjalnego woluminu. W przypadku tworzenia kopii zapasowych komputerów z tymi systemami operacyjnymi należy zawsze wybierać obie opcje: **[SYSTEM]** i **[BOOT]**.

Ponieważ zasady tworzenia kopii zapasowych są powszechnie stosowane do wielu komputerów z różnymi systemami operacyjnymi, firma Acronis zaleca wybieranie zawsze obu woluminów (systemowego i startowego) w celu utworzenia kopii zapasowej — zapewnia to integralność każdego z systemów operacyjnych.

Uwaga dotycząca komputerów z systemem Linux

W określonych scentralizowanych zasadach tworzenia kopii zapasowych można uwzględnić zarówno woluminy (partycje) systemu Windows, jak i systemu Linux.

Na przykład można skonfigurować zasady tworzenia kopii zapasowych woluminu **C:** na komputerach z systemem Windows oraz partycji **/dev/hda1** na komputerach z systemem Linux.

W systemie Linux, w odróżnieniu od systemu Windows, nie ma wyraźnej różnicy między woluminem (partycją) a folderem (katalogiem). W systemie Linux istnieje partycja główna (oznaczona jako /), do której są podłączone (zamontowane) elementy różnego typu, w tym dyski twarde, katalogi i urządzenia systemowe, tworząc drzewo przypominające strukturę plików i folderów systemu Windows.

Załóżmy na przykład, że na komputerze z systemem Linux znajduje się dysk twardy podzielony na trzy woluminy, czyli partycje: pierwszą, drugą i trzecią. Partycje te są dostępne w drzewie odpowiednio jako /dev/hda1, /dev/hda2 i /dev/hda3. Aby utworzyć kopię zapasową trzeciej partycji, w wierszu w oknie dialogowym **Reguły wyboru woluminów do kopii zapasowej** należy wpisać /dev/hda3.

Ponadto partycję sytemu Linux można zamontować w dowolnym miejscu drzewa. Na przykład partycja /dev/hda3 może być zamontowana jako „podkatalog” w drzewie, np. /home/usr/docs. W takim przypadku, aby utworzyć kopię zapasową trzeciej partycji, w polu Wolumin można wpisać /dev/hda3 lub /home/usr/docs.

Ogólnie rzecz biorąc, konfigurując scentralizowane zasady tworzenia kopii zapasowych woluminów na komputerach z systemem Linux, w polu Wolumin należy wprowadzić ścieżki odpowiadające partycjom (takie jak /dev/hda2 lub /home/usr/docs z poprzedniego przykładu), a nie katalogom.

Standardowe nazwy partycji systemu Linux

Nazwy, takie jak /dev/hda1, odzwierciedlają standardowy sposób nadawania nazw partycjom dysków twardych IDE w systemie Linux. Przedrostek hd oznacza typ dysku (IDE), „a” oznacza pierwszy dysk twardy IDE w systemie, a 1 — pierwszą partycję na tym dysku.

Ogólnie standardowa nazwa partycji systemu Linux ma trzy składowe:

- typ dysku: hd (dyski IDE), sd (dyski SCSI), md (programowe dyski RAID, na przykład woluminy dynamiczne);
- numer dysku: „a” dla pierwszego dysku, „b” dla drugiego dysku itd.;
- numer partycji na dysku: 1 dla pierwszej partycji, 2 dla drugiej partycji itd.

Aby zagwarantować tworzenie kopii zapasowych wybranych dysków niezależnie od ich typu, w oknie dialogowym **Reguły wyboru woluminów do kopii zapasowej** należy dodać trzy wpisy, po jednym dla każdego z możliwych typów. Aby na przykład utworzyć kopię zapasową pierwszego dysku twardego na każdym komputerze z systemem Linux podlegającym zasadom scentralizowanym, w polu Wolumin należy wpisać następujące wiersze:

/dev/hda1

/dev/sda1

/dev/mda1

Nazwy woluminów logicznych

Aby utworzyć kopie zapasowe woluminów logicznych, nazywanych również woluminami LVM, określ ich pełne nazwy w regułach wyboru. Pełna nazwa woluminu logicznego obejmuje grupę woluminów, do której on należy.

Aby na przykład utworzyć kopie zapasowe dwóch woluminów logicznych: **lv_root** i **lv_bin**, które oba należą do grupy woluminów **vg_mymachine**, określ następujące reguły wyboru:

```
/dev/vg_mymachine/lv_root
/dev/vg_mymachine/lv_bin
```

W celu wyświetlenia listy woluminów logicznych na komputerze użyj narzędzia **lvdisplay**. W naszym przykładzie dane wyjściowe będą podobne do następujących:

```
--- Logical volume ---
LV Name          /dev/vg_mymachine/lv_root
VG Name          vg_mymachine
…

--- Logical volume ---
LV Name          /dev/vg_mymachine/lv_bin
VG Name          vg_mymachine
…
```

Wskazówka: *Aby móc automatycznie tworzyć informacje o strukturze woluminów podczas odzyskiwania, upewnij się, że dla każdego komputera do tworzenia kopii zapasowej został wybrany wolumin zawierający katalog* ***/etc/Acronis****. Aby uzyskać więcej informacji, zobacz „Zapisywanie informacji o strukturze woluminu” (s. 52).*

Reguły wyboru plików do kopii zapasowej

Zdefiniuj reguły wyboru plików. Na podstawie tych reguł będą tworzone kopie zapasowe plików i/lub folderów na komputerach, na których zostaną zastosowane zasady.

Aby zdefiniować reguły wyboru plików

W pierwszym wierszu wybierz regułę na liście lub wpisz ją ręcznie. Aby dodać kolejną regułę, kliknij kolejny pusty wiersz i wybierz regułę na liście lub wpisz ją ręcznie.

Program zapamiętuje reguły wpisane ręcznie, dlatego następnym razem po otwarciu okna reguły te będą dostępne na liście razem z regułami domyślnymi.

Windows

Pełna ścieżka

Wskaż foldery i pliki do utworzenia kopii zapasowej. Jeśli określisz dokładną ścieżkę do pliku lub folderu, zasady spowodują utworzenie kopii zapasowej tego elementu na wszystkich komputerach, na których ta dokładna ścieżka zostanie znaleziona.

Elementy uwzględniane	W kolumnie Pliki i foldery wpisz lub wybierz:
Plik Text.doc w folderze D:\Work	**D:\Work\Text.doc**
Folder C:\Windows	**C:\Windows**

Zmienne środowiskowe

Niektóre zmienne środowiskowe wskazują foldery systemu Windows. Korzystanie z takich zmiennych zamiast pełnych ścieżek do plików i folderów gwarantuje, że kopia zapasowa właściwych folderów systemu Windows zostanie utworzona niezależnie od lokalizacji systemu Windows na konkretnym komputerze.

Elementy uwzględniane	W kolumnie Pliki i foldery wpisz lub wybierz	Komentarze
Folder Program Files	**%PROGRAMFILES%**	Wskazuje folder Program Files (na przykład **C:\Program Files**)
Folder systemu Windows	**%WINDIR%**	Wskazuje folder, w którym znajdują się pliki systemu Windows (na przykład **C:\Windows**)
Typowe dane dotyczące wszystkich profilów użytkowników	**%ALLUSERSPROFILE%**	Wskazuje folder, w którym znajdują się typowe dane dotyczące wszystkich profilów użytkowników (zwykle **C:\Documents and Settings\All Users** w systemie Windows XP i **C:\ProgramData** w systemie Windows Vista)

Można korzystać z innych zmiennych środowiskowych lub łączyć zmienne środowiskowe i tekst. Na przykład, aby odwołać się na komputerach do folderu Acronis znajdującego się w folderze Program Files, wpisz: **%PROGRAMFILES%\Acronis**

Szablony

Szablony przypominają zmienne środowiskowe, ale są już wstępnie dostosowane.

Elementy uwzględniane	W kolumnie Pliki i foldery wpisz lub wybierz:	Komentarze
Wszystkie pliki we wszystkich woluminach na komputerze	**[Wszystkie pliki]**	Wskazuje wszystkie pliki we wszystkich woluminach na komputerze.
Wszystkie profile użytkowników istniejące na komputerze	**[Wszystkie foldery profilów]**	Wskazuje folder, w którym znajdują się wszystkie profile użytkowników (zwykle **C:\Documents and Settings** w systemie Windows XP i **C:\Users** w systemie Windows Vista).

Linux

Elementy uwzględniane	W kolumnie Pliki i foldery wpisz lub wybierz:
Plik tekstowy file.txt w woluminie /dev/hda3 zamontowanym na /home/usr/docs	**/dev/hda3/file.txt** lub **/home/usr/docs/file.txt**
Katalog główny typowych użytkowników	**/home**
Katalog główny użytkownika root	**/root**
Katalog dla wszystkich programów użytkowników	**/usr**
Katalog plików konfiguracyjnych systemu	**/etc**

7.3.3 Poświadczenia dostępu dla źródła

Określ poświadczenia wymagane do uzyskania dostępu do danych wybranych do kopii zapasowej.

Aby określić poświadczenia

1. Wybierz jedną z następujących opcji:
   - **Użyj poświadczeń zasad**

     Program uzyska dostęp do źródła danych, korzystając z poświadczeń konta zasad tworzenia kopii zapasowych, które zostały określone w sekcji Ogólne.
   - **Użyj następujących poświadczeń**

     Program uzyska dostęp do źródła danych, korzystając z poświadczeń określonych przez użytkownika. Z tej opcji należy korzystać, jeśli poświadczenia zasad nie mają uprawnień dostępu do danych.

     Określ:
     - **Nazwa użytkownika**. Wprowadzając nazwę konta użytkownika usługi Active Directory, należy określić również nazwę domeny (DOMENA\Nazwa_użytkownika lub Nazwa_użytkownika@domena).
     - **Hasło**. Hasło dla konta.
2. Kliknij **OK**.

7.3.4 Wykluczenia

Skonfiguruj wykluczenia, określając konkretne typy plików nie uwzględnianych w kopii zapasowej. Z przechowywania w archiwum można wykluczyć na przykład bazę danych, pliki i foldery ukryte oraz systemowe, a także pliki z określonymi rozszerzeniami.

Aby określić pliki i foldery do wykluczenia:

Skonfiguruj dowolne z następujących parametrów:

- **Wyklucz wszystkie ukryte pliki i foldery**

  Opcja ta działa tylko w systemach plików obsługiwanych przez system Windows. Zaznacz to pole wyboru, aby pominąć pliki i foldery z atrybutem **Ukryty**. Jeśli folder jest **ukryty**, program wykluczy całą jego zawartość, w tym również pliki, które nie mają atrybutu **Ukryty**.
- **Wyklucz wszystkie pliki i foldery systemowe**

  Opcja ta działa tylko w systemach plików obsługiwanych przez system Windows. Zaznacz to pole wyboru, aby pominąć pliki i foldery z atrybutem **Systemowy**. Jeśli folder jest **systemowy**, program wykluczy całą jego zawartość, w tym również pliki, które nie mają atrybutu **Systemowy**.

*Atrybuty plików i folderów można sprawdzić w ich właściwościach lub używając polecenia **attrib**. Więcej informacji można znaleźć w Centrum pomocy i obsługi technicznej w systemie Windows.*

- **Wyklucz pliki spełniające następujące kryteria**

  Zaznacz to pole wyboru, aby pominąć pliki i foldery, których nazwy pasują do podanych na liście kryteriów zwanych maskami plików. Aby utworzyć listę masek plików, użyj przycisków **Dodaj**, **Edytuj**, **Usuń** i **Usuń wszystko**.

  W masce plików można użyć jednego lub kilku symboli wieloznacznych * i ?:

  Gwiazdka (*) zastępuje dowolną liczbę znaków w nazwie pliku (w tym również zero). Na przykład maska Dok*.txt zwraca pliki takie jak Dok.txt i Dokument.txt.

  Znak zapytania (?) zastępuje dokładnie jeden znak w nazwie pliku. Na przykład maska Dok?.txt zwraca pliki takie jak Dok1.txt i Doku.txt, ale nie zwraca plików Dok.txt ani Dok11.txt.

Aby wykluczyć folder określony przez ścieżkę zawierającą literę dysku, dodaj ukośnik odwrotny (\) do nazwy folderu w kryterium, np.: C:\Finanse\

Przykłady wykluczeń

Kryterium	Przykład	Opis
Windows i Linux		
Według nazwy	F.log F	Wyklucza wszystkie pliki o nazwie „F.log”. Wyklucza wszystkie foldery o nazwie „F”.
Według maski (*)	*.log F*	Wyklucza wszystkie pliki z rozszerzeniem .log. Wyklucza wszystkie pliki i foldery, których nazwa rozpoczyna się od litery „F” (np. foldery F, F1 i pliki F.log, F1.log).
Według maski (?)	F???.log	Wyklucza wszystkie pliki z rozszerzeniem .log, których nazwy składają się z czterech znaków i zaczynają od litery „F”.
Windows		

Według ścieżki pliku	C:\Finanse\F.log	Wyklucza plik „F.log” znajdujący się w folderze C:\Finanse.
Według ścieżki folderu	C:\Finanse\F\	Wyklucza folder C:\Finanse\F (należy określić pełną ścieżkę, rozpoczynającą się od litery dysku).
Linux		
Według ścieżki pliku	/home/user/Finanse/F.log	Wyklucza plik „F.log” znajdujący się w folderze /home/user/Finanse.
Według ścieżki folderu	/home/user/Finanse/	Wyklucza folder /home/user/Finanse.

7.3.5 Archiwum

Określ miejsce docelowe archiwów i zdefiniuj nazwy nowych archiwów kopii zapasowych.

1. Wybór miejsca docelowego archiwów

Wybierz miejsce przechowywania archiwów komputerów:

- Przechowuj archiwa wszystkich komputerów w jednej lokalizacji
  - Aby utworzyć kopię zapasową danych w magazynie Acronis Online Backup Storage, kliknij **Zaloguj** i określ poświadczenia logowania do magazynu online. Następnie rozwiń grupę **Magazyn kopii zapasowych online** i wybierz konto.

    Przed utworzeniem kopii zapasowej w magazynie online należy zakupić subskrypcję usługi tworzenia kopii zapasowych online oraz aktywować tę subskrypcję na komputerach, których kopię zapasową chcesz utworzyć. Usługa tworzenia kopii zapasowych online jest niedostępna w systemie Linux.

  Usługa Acronis Backup & Recovery 10 Online nie jest dostępna we wszystkich regionach. Aby uzyskać więcej informacji, kliknij tutaj: http://www.acronis.pl/my/backup-recovery-online/.

  - Aby przechowywać archiwa w skarbcu centralnym, rozwiń grupę Scentralizowane i kliknij skarbiec.
  - Aby przechowywać archiwa w udziale sieciowym, rozwiń grupę Foldery sieciowe, wybierz żądany komputer sieciowy, a następnie kliknij folder udostępniony. Jeśli udział sieciowy wymaga poświadczeń dostępu, program wyświetli odpowiedni monit.
  - Aby przechowywać archiwa na serwerze FTP lub SFTP, rozwiń odpowiednią grupę i kliknij odpowiedni serwer, a następnie wybierz folder, w którym będą przechowywane archiwa.

  Jak wynika z oryginalnej specyfikacji protokołu FTP, poświadczenia wymagane do uzyskania dostępu do serwerów FTP są przesyłane w sieci jako otwarty tekst. Oznacza to, że nazwę użytkownika i hasło można przejąć przy użyciu programu do przechwytywania pakietów.

- Przechowuj archiwum każdego komputera w określonym folderze na komputerze

  W polu Ścieżka wprowadź pełną ścieżkę do folderu. Folder o określonej ścieżce zostanie utworzony na każdym komputerze, którego będą dotyczyć zasady.
- Przechowuj archiwum każdego komputera w jego strefie Acronis Secure Zone

  Strefę Acronis Secure Zone należy utworzyć na każdym komputerze, na którym zostaną zastosowane zasady. Aby uzyskać informacje dotyczące sposobu tworzenia strefy Acronis Secure Zone, zobacz Tworzenie strefy Acronis Secure Zone (s. 286).

2. Nadawanie nazw archiwom

Kopia zapasowa danych z każdego komputera zostanie utworzona w oddzielnym archiwum. Należy określić nazwy archiwów.

Program wygeneruje typową nazwę nowych archiwów i wyświetli ją w polu Nazwa. Jest to nazwa w postaci [NazwaZasad]_[NazwaKomputera]_Archiwum1. Jeśli automatycznie wygenerowana nazwa jest nieodpowiednia, określ inną.

Po wybraniu opcji Przechowuj archiwa wszystkich komputerów w jednej lokalizacji należy korzystać ze zmiennych, aby zapewnić unikatowość nazw archiwów w danej lokalizacji.

1. Kliknij Dodaj zmienne, a następnie wybierz opcję:
   - [Nazwa komputera] — podstawienie za nazwę komputera
   - [Nazwa zasad] — podstawienie za nazwę zasad tworzenia kopii zapasowych

   W efekcie w polu Nazwa pojawi się następująca reguła: [Nazwa komputera]_[Nazwa zasad]_Archiwum1

   Załóżmy, że zasady tworzenia kopii zapasowej o nazwie KOPIA_SYSTEMU zostaną zastosowane na trzech komputerach (DZIALFIN1, DZIALFIN2, DZIALFIN3). W lokalizacji zostaną utworzone trzy archiwa:

   DZIALFIN1_KOPIA_SYSTEMU_Archiwum1

   DZIALFIN2_KOPIA_SYSTEMU_Archiwum1

   DZIALFIN3_KOPIA_SYSTEMU_Archiwum1
2. Kliknij OK.

Nazwa ma postać ArchiwumN, gdzie N to numer kolejnego archiwum. Jeśli w danej lokalizacji istnieje już archiwum Archiwum1, program automatycznie zasugeruje nazwę Archiwum2.

7.3.6 Poświadczenia dostępu dla lokalizacji

Określ poświadczenia dostępu do lokalizacji, w której będzie przechowywane archiwum kopii zapasowej. Nazwa użytkownika takich poświadczeń będzie oznaczać właściciela archiwum.

Aby określić poświadczenia

1. Wybierz jedną z następujących opcji:
   - **Użyj poświadczeń zasad**

     Program uzyska dostęp do lokalizacji, korzystając z poświadczeń zasad tworzenia kopii zapasowych, które zostały określone w sekcji Ogólne.
   - **Użyj następujących poświadczeń**

     Program uzyska dostęp do lokalizacji, korzystając z poświadczeń określonych przez użytkownika. Z tej opcji należy korzystać, jeśli poświadczenia zasad nie mają uprawnień dostępu do lokalizacji. Być może trzeba będzie określić specjalne poświadczenia dla udziału sieciowego lub węzła magazynowania.

     Określ:
     - **Nazwa użytkownika**. Wprowadzając nazwę konta użytkownika usługi Active Directory, należy określić również nazwę domeny (DOMENA\Nazwa_użytkownika lub Nazwa_użytkownika@domena).
     - **Hasło**. Hasło dla konta.
2. Kliknij **OK**.

Ostrzeżenie: *Jak wynika z oryginalnej specyfikacji protokołu FTP, poświadczenia wymagane do uzyskania dostępu do serwerów FTP są przesyłane w sieci jako otwarty tekst. Oznacza to, że nazwę użytkownika i hasło można przejąć przy użyciu programu do przechwytywania pakietów.*

7.3.7 Wybór schematu tworzenia kopii zapasowych

Wybierz jeden z dostępnych schematów tworzenia kopii zapasowych:

- **Utwórz kopię zapasową** — aby utworzyć zadanie tworzenia kopii zapasowej przeznaczone do ręcznego uruchamiania oraz uruchomić to zadanie natychmiast po utworzeniu.
- **Utwórz kopię zapasową później** — aby utworzyć zadanie tworzenia kopii zapasowej przeznaczone do ręcznego uruchamiania LUB zaplanować jednorazowe wykonanie zadania w przyszłości.
- **Prosty** — aby zaplanować czas i częstotliwość tworzenia kopii zapasowych danych oraz określić reguły przechowywania.
- **Dziadek-ojciec-syn** — aby użyć schematu tworzenia kopii zapasowych Dziadek-ojciec-syn. Schemat ten umożliwia tworzenie kopii zapasowej danych najwyżej raz dziennie. Użytkownik wyznacza dni wykonywania dziennej kopii zapasowej i spośród tych dni wybiera dzień tworzenia kopii tygodniowej/miesięcznej. Następnie ustawia okresy przechowywania kopii zapasowych dziennych (zwanych „synami"), tygodniowych (zwanych „ojcami") i miesięcznych (zwanych „dziadkami"). Nieaktualne kopie zapasowe będą usuwane automatycznie.
- **Wieża Hanoi** — aby użyć schematu tworzenia kopii zapasowych Wieża Hanoi, w którym użytkownik planuje czas i częstotliwość tworzenia kopii zapasowych (sesje) oraz wybiera liczbę poziomów kopii (maksymalnie 16). W tym schemacie kopie zapasowe można wykonywać częściej niż raz dziennie. Konfigurując schemat i wybierając poziomy tworzenia kopii zapasowych, automatycznie uzyskuje się okres wycofywania, czyli gwarantowaną liczbę sesji, o którą można się cofnąć w dowolnym momencie. Mechanizm automatycznego czyszczenia umożliwia zachowanie wymaganego okresu wycofywania dzięki usuwaniu nieaktualnych kopii zapasowych i zachowywaniu najnowszych kopii na każdym poziomie.
- **Niestandardowy** — aby utworzyć schemat tworzenia kopii zapasowych, w którym użytkownik może dowolnie konfigurować strategię tworzenia kopii w sposób najlepiej odpowiadający potrzebom przedsiębiorstwa. Można zdefiniować wiele harmonogramów dla różnych typów kopii zapasowych, dodać warunki i określić reguły przechowywania.
- **Pierwotna kopia zapasowa w magazynie** — aby zapisać lokalnie pełną kopię zapasową, której ostatecznym miejscem docelowym jest magazyn Acronis Online Backup Storage.

Schemat tworzenia kopii zapasowych

W schemacie **Utwórz kopię zapasową** kopia zapasowa zostanie wykonana niezwłocznie po kliknięciu przycisku **OK** u dołu strony.

W polu **Typ kopii zapasowej** wybierz, czy utworzyć pełną, przyrostową lub różnicową kopię zapasową (s. 36).

Schemat późniejszego tworzenia kopii zapasowych

W schemacie „Utwórz kopię zapasową później" kopia zapasowa zostanie utworzona tylko raz — o godzinie i w dniu określonym przez użytkownika.

Określ właściwe ustawienia w następujący sposób

Typ kopii zapasowej	Wybierz typ kopii zapasowej: pełna, przyrostowa lub różnicowa. Jeśli archiwum nie zawiera pełnej kopii zapasowej, zostanie ona utworzona niezależnie od dokonanego wyboru.
Data i godzina	Określ początek tworzenia kopii zapasowej.
Zadanie zostanie uruchomione ręcznie	Zaznacz to pole wyboru, jeśli nie chcesz dołączyć zadania do harmonogramu i zamierzasz uruchomić je ręcznie później.

Prosty schemat

W schemacie prostym wystarczy zaplanować czas i częstotliwość tworzenia kopii zapasowej danych oraz zdefiniować regułę przechowywania. Za pierwszym razem zostanie utworzona pełna kopia zapasowa. Następne kopie zapasowe będą przyrostowe.

Aby skonfigurować prosty schemat tworzenia kopii zapasowych, określ właściwe ustawienia w następujący sposób:

Kopia zapasowa	Skonfiguruj harmonogram tworzenia kopii zapasowych — czas i częstotliwość wykonywania kopii zapasowej danych. Aby dowiedzieć się więcej na temat konfigurowania harmonogramu, zobacz sekcję Tworzenie harmonogramu (s. 185).
Reguła przechowywania	W schemacie prostym dostępna jest tylko jedna reguła przechowywania (s. 45). Zdefiniuj okres przechowywania kopii zapasowych.

Schemat Dziadek-ojciec-syn

W skrócie

- Dzienne przyrostowe, tygodniowe różnicowe i miesięczne pełne kopie zapasowe
- Wybór dnia tworzenia tygodniowych i miesięcznych kopii zapasowych
- Wybór okresów przechowywania kopii zapasowych każdego typu

Opis

Załóżmy, że chcemy skonfigurować plan tworzenia kopii zapasowych, w ramach którego regularnie wykonywane będą dzienne (D), tygodniowe (T) i miesięczne (M) kopie zapasowe. Oto najprostszy sposób: poniższa tabela przedstawia przykładowy dwumiesięczny okres takiego planu.

	Pn	Wt	Śr	Cz	Pt	Sb	Nd
1 sty–7 sty	D	D	D	D	T	-	-
8 sty–14 sty	D	D	D	D	T	-	-
15 sty–21 sty	D	D	D	D	T	-	-
22 sty–28 sty	D	D	D	D	M	-	-
29 sty–4 lut	D	D	D	D	T	-	-
5 lut–11 lut	D	D	D	D	T	-	-
12 lut–18 lut	D	D	D	D	T	-	-
19 lut–25 lut	D	D	D	D	M	-	-
26 lut–4 mar	D	D	D	D	T	-	-

Dzienne kopie zapasowe są wykonywane każdego dnia z wyjątkiem piątku, który został wyznaczony na tworzenie tygodniowych i miesięcznych kopii zapasowych. Miesięczne kopie zapasowe są wykonywane co czwarty piątek, natomiast tygodniowe kopie zapasowe we wszystkie pozostałe piątki.

- Miesięczne kopie zapasowe („dziadek”) to kopie pełne.
- Tygodniowe kopie zapasowe („ojciec”) to kopie różnicowe.
- Dzienne kopie zapasowe („syn”) to kopie przyrostowe.

Parametry

W schemacie Dziadek-ojciec-syn (GFS) można skonfigurować poniższe parametry.

Rozpocznij tworzenie kopii zapasowej o:	Określa godzinę rozpoczęcia tworzenia kopii zapasowej. Wartość domyślna to 12:00.
Utwórz kopię zapasową dnia:	Określa dni wykonywania kopii zapasowej. Wartość domyślna to dni robocze.
Tygodniowa/miesięczna:	Określa dzień spośród dni wybranych w polu **Utwórz kopię zapasową** dnia, który jest zarezerwowany na tworzenie tygodniowych i miesięcznych kopii zapasowych. Miesięczna kopia zapasowa będzie wykonywana co czwarty taki dzień. Wartość domyślna to piątek.
Zachowuj kopie zapasowe:	Określa czas przechowywania kopii zapasowych w archiwum. Czas przechowywania można określić w godzinach, dniach, tygodniach, miesiącach lub latach. Miesięczne kopie zapasowe można przechowywać bez ograniczeń czasowych, wybierając opcję **Zachowaj w nieskończoność**. Poniżej znajdują się wartości domyślne dla każdego typu kopii zapasowej. Dzienna: 7 dni (zalecane minimum) Tygodniowa: 4 tygodnie Miesięczna: w nieskończoność Okres przechowywania tygodniowych kopii zapasowych musi być dłuższy niż okres przechowywania kopii dziennych. Okres przechowywania miesięcznych kopii zapasowych musi być dłuższy niż okres przechowywania kopii tygodniowych. Zaleca się przynajmniej jednotygodniowy okres przechowywania dziennych kopii zapasowych.
Ustawienia zaawansowane:	Aby określić Zaawansowane ustawienia harmonogramu (s. 195), kliknij **Zmień** w obszarze **Ustawienia zaawansowane**.

Niezależnie od ustawień kopia zapasowa nie zostanie usunięta, dopóki nie zostaną usunięte jej wszystkie kopie zależne. Dlatego tygodniowe lub miesięczne kopie zapasowe mogą pozostawać w archiwum przez kilka dni po spodziewanej dacie utraty ważności.

Jeśli harmonogram rozpoczyna się od dziennej lub tygodniowej kopii zapasowej, zamiast niej zostanie utworzona pełna kopia zapasowa.

Przykłady

Każdy dzień ostatniego tygodnia, każdy tydzień ostatniego miesiąca

Rozważmy schemat tworzenia kopii zapasowych Dziadek-ojciec-syn, który może okazać się przydatny w wielu sytuacjach.

- Kopie zapasowe plików tworzone codziennie, w tym w sobotę i niedzielę
- Zapewnienie możliwości odzyskania plików do stanu na dowolny z ostatnich siedmiu dni
- Zapewnienie dostępu do tygodniowych kopii zapasowych ostatniego miesiąca
- Zachowywanie miesięcznych kopii zapasowych w nieskończoność

Parametry schematu tworzenia kopii zapasowych można skonfigurować w następujący sposób:

- Rozpocznij tworzenie kopii zapasowej o: **23.00**
- Utwórz kopię zapasową dnia: **Wszystkie dni**
- Tygodniowa/miesięczna: **Sobota** (przykładowo)
- Zachowuj kopie zapasowe:
  - Codzienna: **1 tydzień**
  - Tygodniowa: **1 miesiąc**
  - Miesięczna: **w nieskończoność**

W wyniku tych ustawień zostanie utworzone archiwum codziennych, tygodniowych i miesięcznych kopii zapasowych. Codzienne kopie zapasowe będą dostępne przez siedem dni od momentu ich utworzenia. Codzienna kopia zapasowa utworzona np. w niedzielę 1 stycznia będzie dostępna do następnej niedzieli 8 stycznia. Pierwsza tygodniowa kopia zapasowa utworzona w sobotę 7 stycznia będzie przechowywana w systemie do 7 lutego. Miesięczne kopie zapasowe nie zostaną nigdy usunięte.

Ograniczone miejsce przechowywania

Aby nie przeznaczać dużej ilości miejsca na ogromne archiwum, schemat Dziadek-ojciec-syn (GFS) można skonfigurować tak, aby krócej przechowywać kopie zapasowe, a jednocześnie zapewnić odzyskanie danych w razie ich przypadkowej utraty.

Przyjmijmy następujące założenia:

- kopie zapasowe mają być wykonywane na koniec każdego dnia roboczego;
- musi istnieć możliwość odzyskania przypadkowo usuniętego lub nieumyślnie zmodyfikowanego pliku, jeśli zostało to wykryte relatywnie szybko;
- dostęp do tygodniowej kopii zapasowej musi być zapewniony przez 10 dni od momentu jej utworzenia;
- miesięczne kopie zapasowe muszą być zachowywane przez pół roku.

Parametry schematu tworzenia kopii zapasowych można skonfigurować w następujący sposób:

- Rozpocznij tworzenie kopii zapasowej o: **18.00**
- Utwórz kopię zapasową dnia: **Dni robocze**
- Tygodniowa/miesięczna: **piątek**
- Zachowuj kopie zapasowe:
  - Codzienna: **1 tydzień**
  - Tygodniowa: **10 dni**
  - Miesięczna: **6 miesięcy**

W tym schemacie użytkownik ma tydzień na odzyskanie poprzedniej wersji uszkodzonego pliku z codziennej kopii zapasowej, a także 10-dniowy dostęp do tygodniowych kopii zapasowych. Każda miesięczna pełna kopia zapasowa będzie dostępna przez sześć miesięcy od daty jej utworzenia.

Harmonogram prac

Załóżmy, że jesteś konsultantem finansowym i pracujesz w firmie na pół etatu we wtorki i czwartki. W te dni dokonujesz zmian w dokumentach i sprawozdaniach finansowych, aktualizujesz arkusze kalkulacyjne itp. na komputerze przenośnym. Aby utworzyć kopie zapasowe tych danych możesz:

- Śledzić zmiany w sprawozdaniach finansowych, arkuszach kalkulacyjnych itp. we wtorki i czwartki (codzienna przyrostowa kopia zapasowa).
- Sporządzać tygodniowe podsumowania zmian plików w porównaniu z ostatnim miesiącem (tygodniowa różnicowa kopia zapasowa w każdy piątek).
- Raz na miesiąc robić pełną kopię zapasową plików.

Ponadto załóżmy, że chcesz zachować wszystkie kopie zapasowe — w tym dzienne — przez co najmniej sześć miesięcy.

Do tych celów odpowiedni jest następujący schemat „dziadek-ojciec-syn” (GFS):

- Rozpocznij tworzenie kopii zapasowej o: **23:30**
- Utwórz kopię zapasową dnia: **wtorek, czwartek, piątek**
- Tygodniowa/miesięczna: **piątek**
- Zachowuj kopie zapasowe:
  - Codzienna: **6 miesięcy**
  - Tygodniowa: **6 miesięcy**
  - Miesięczna: **5 lat**

W tym przykładzie dzienne przyrostowe kopie zapasowe będą wykonywane we wtorki i czwartki, natomiast kopie tygodniowe i miesięczne w piątki. Uwaga: aby wybrać **piątek** w polu **Tygodniowa/miesięczna**, trzeba najpierw zaznaczyć ten dzień w polu **Utwórz kopię zapasową dnia**.

Takie archiwum umożliwi porównanie dokumentów finansowych na pierwszy i ostatni dzień pracy oraz utworzenie pięcioletniej historii wszystkich dokumentów itp.

Bez dziennych kopii zapasowych

Przeanalizujmy bardziej egzotyczny schemat „dziadek-ojciec-syn” (GFS):

- Rozpocznij tworzenie kopii zapasowej o: **12.00 w południe**
- Utwórz kopię zapasową dnia: **piątek**
- Tygodniowa/miesięczna: **piątek**
- Zachowuj kopie zapasowe:
  - Codzienna: **1 tydzień**
  - Tygodniowa: **1 miesiąc**
  - Miesięczna: **w nieskończoność**

Zatem kopie zapasowe będą wykonywane w piątki. W ten sposób piątek będzie jedynym dniem tworzenia tygodniowych i miesięcznych kopii zapasowych, bez wyboru dnia dla kopii dziennych. Tak więc powstałe archiwum „dziadek-ojciec” będzie składać się tylko z tygodniowych kopii różnicowych i miesięcznych pełnych kopii zapasowych.

Chociaż można użyć schematu „dziadek-ojciec-syn” do utworzenia takiego archiwum, w tej sytuacji schemat niestandardowy zapewni większą elastyczność.

Schemat Wieża Hanoi

W skrócie

- Maksymalnie 16 poziomów pełnych, różnicowych i przyrostowych kopii zapasowych.
- Kopie zapasowe kolejnego poziomu występują dwa razy rzadziej niż kopie zapasowe poprzedniego poziomu.
- Jednocześnie jest przechowywana tylko jedna kopia zapasowa każdego poziomu.
- Większe zagęszczenie nowszych kopii zapasowych.

Parametry

Można skonfigurować następujące parametry schematu Wieża Hanoi:

Harmonogram	Skonfiguruj harmonogram codzienny (s. 186), tygodniowy (s. 188) lub miesięczny (s. 190). Konfiguracja parametrów harmonogramu umożliwia tworzenie harmonogramów prostych (przykład prostego harmonogramu codziennego: zadanie tworzenia kopii zapasowej uruchamiane codziennie o 10.00) oraz harmonogramów bardziej złożonych (przykład złożonego harmonogramu codziennego: zadanie uruchamiane co trzy dni, począwszy od 15 stycznia. Zadanie będzie powtarzane w określone dni co dwie godziny od 10.00 do 22.00). W ten sposób harmonogram złożony określa sesje, podczas których schemat będzie stosowany. W omówieniu znajdującym się poniżej pojęcie „dni” można zastąpić terminem „sesje zaplanowane”.
Liczba poziomów	Wybierz od 2 do 16 poziomów tworzenia kopii zapasowych. Zobacz szczegółowy przykład poniżej.
Okres wycofywania	Gwarantowana liczba sesji, podczas których można przywrócić kopie z archiwum w dowolnym momencie. Obliczana jest automatycznie na podstawie parametrów harmonogramu i liczby poziomów określonych przez użytkownika. Zobacz szczegółowy przykład poniżej.

Przykład

Parametry **harmonogramu** są następujące

- Powtarzaj co: 1 dzień
- Częstotliwość: Raz o 18.00

Liczba poziomów: 4

Pierwsze 14 dni (lub 14 sesji) harmonogramu tego schematu będą wyglądały jak poniżej. Liczby zacienione oznaczają poziomy tworzenia kopii zapasowych.

1	2	3	4	5	6	7	8	9	10	11	12	13	14
4	1	2	1	3	1	2	1	4	1	2	1	3	1

Kopie zapasowe różnych poziomów są różnego typu:

- kopie zapasowe *ostatniego poziomu* (w tym przypadku poziom 4) to kopie pełne;
- kopie zapasowe *średniego poziomu* (2, 3) to kopie różnicowe;
- kopie zapasowe *pierwszego poziomu* (1) to kopie przyrostowe.

Zastosowanie mechanizmu czyszczenia umożliwia zachowanie tylko najnowszych kopii zapasowych każdego poziomu. W dniu 8 — dzień przed utworzeniem nowej pełnej kopii zapasowej — archiwum będzie wyglądało następująco.

1	2	3	4	5	6	7	8
4	1	2	1	3	1	2	1

Ten schemat zapewnia wydajne przechowywanie danych: więcej kopii zapasowych jest skumulowanych w okolicach aktualnego czasu. Mając cztery kopie zapasowe, można odzyskać dane zapisane dziś, wczoraj, w połowie tygodnia lub tydzień temu.

Okres wycofywania

Liczba dni, podczas których można powracać do kopii zapasowych znajdujących się w archiwum, jest inna w różne dni. Minimalną zagwarantowaną liczbę dni nazywa się okresem wycofywania.

Tabela poniżej pokazuje okresy tworzenia i wycofywania kopii zapasowych dla schematów z różnymi poziomami.

Liczba poziomów	**Pełna kopia zapasowa co**	**W zależności od dnia można powrócić**	**Okres wycofywania**
2	2 dni	od 1 do 2 dni	1 dzień
3	4 dni	od 2 do 5 dni	2 dni
4	8 dni	od 4 do 11 dni	4 dni
5	16 dni	od 8 do 23 dni	8 dni
6	32 dni	od 16 do 47 dni	16 dni

Dodanie poziomu powoduje podwojenie okresów tworzenia pełnej kopii zapasowej oraz wycofywania.

Wróćmy do poprzedniego przykładu, aby zobaczyć, dlaczego liczba dni odzyskiwania się zmienia.

Oto kopie zapasowe w dniu 12 (liczby w kolorze szarym oznaczają usunięte kopie zapasowe).

1	2	3	4	5	6	7	8	9	10	11	12
4	1	2	1	3	1	2	1	4	1	2	1

Nowa różnicowa kopia zapasowa na poziomie 3 jeszcze nie została utworzona, zatem kopia dnia piątego jest nadal przechowywana. Jest ona zależna od pełnej kopii zapasowej dnia pierwszego, dlatego jest również dostępna. Dzięki temu możemy cofnąć się aż o 11 dni, co jest najlepszym scenariuszem w tym przypadku.

Jednak w następnym dniu zostanie utworzona nowa różnicowa kopia zapasowa trzeciego poziomu, a stara pełna kopia zapasowa zostanie usunięta.

1	2	3	4	5	6	7	8	9	10	11	12	13
4	1	2	1	3	1	2	1	4	1	2	1	3

To daje zaledwie czterodniowy okres na odzyskiwanie danych, co okazuje się być najgorszym scenariuszem w tym przypadku.

W dniu 14 ten okres wynosi pięć dni. W kolejne dni wydłuża się, zanim ponownie zacznie się skracać itd.

1	2	3	4	5	6	7	8	9	10	11	12	13	14
4	1	2	1	3	1	2	1	4	1	2	1	3	1

Parametr Okres wycofywania pokazuje zagwarantowaną liczbę dni na odzyskiwanie danych nawet w najgorszym przypadku. Przy schemacie z czterema poziomami wynosi on cztery dni.

Niestandardowy schemat tworzenia kopii zapasowych

W skrócie

- Niestandardowy harmonogram i warunki tworzenia kopii zapasowych każdego typu
- Niestandardowy harmonogram i reguły przechowywania

Parametry

Parametr	Znaczenie
Pełna kopia zapasowa	Określa harmonogram i warunki wykonywania pełnej kopii zapasowej. Można na przykład tak skonfigurować tworzenie pełnej kopii zapasowej, aby była wykonywana w każdą niedzielę o 1:00 po wylogowaniu się wszystkich użytkowników.
Przyrostowa	Określa harmonogram i warunki wykonywania przyrostowej kopii zapasowej. Jeśli w momencie uruchomienia zadania archiwum nie zawiera pełnych kopii zapasowych, zamiast kopii przyrostowej tworzona jest pełna kopia zapasowa.
Różnicowa	Określa harmonogram i warunki wykonywania różnicowej kopii zapasowej. Jeśli w momencie uruchomienia zadania archiwum nie zawiera pełnych kopii zapasowych, zamiast kopii różnicowej tworzona jest pełna kopia zapasowa.
Czyszczenie archiwum	Określa sposób usuwania starych kopii zapasowych. Dwie dostępne możliwości to regularne stosowanie reguł przechowywania (s. 45) i czyszczenie archiwum po tym, gdy w docelowej lokalizacji zabraknie miejsca. W domyślnej konfiguracji reguły przechowywania nie są określone. Oznacza to, że starsze kopie zapasowe nie zostaną automatycznie usunięte. **Używanie reguł przechowywania** Określ reguły przechowywania i warunki ich stosowania. To ustawienie jest zalecane dla takich lokalizacji kopii zapasowych, jak foldery udostępnione lub skarbce centralne. **Gdy w trakcie tworzenia kopii zapasowej zabraknie miejsca.** Archiwum zostanie wyczyszczone tylko wtedy, gdy podczas tworzenia kopii zapasowej zabraknie miejsca na utworzenie nowej kopii. W takiej sytuacji program wykona następujące czynności: ▪ Usunięcie najstarszej pełnej kopii zapasowej razem ze wszystkimi zależnymi kopiami przyrostowymi/różnicowymi. ▪ Gdy dostępna jest tylko jedna pełna kopia zapasowa, ale trwa wykonywanie pełnej kopii zapasowej, istniejąca pełna kopia zapasowa zostanie usunięta razem ze wszystkimi zależnymi kopiami przyrostowymi/różnicowymi. ▪ Gdy dostępna jest tylko jedna pełna kopia zapasowa, ale trwa wykonywanie przyrostowej lub różnicowej kopii zapasowej, zostanie wyświetlony błąd o braku dostępnego miejsca. Ustawienie to jest zalecane podczas wykonywania kopii zapasowych na pamięć USB lub do strefy Acronis Secure Zone. Ustawienie to nie dotyczy skarbców zarządzanych.

	Ustawienie to umożliwia usunięcie ostatniej kopii zapasowej w archiwum w sytuacji, w której urządzenie pamięci masowej nie może pomieścić więcej niż jednej kopii. Jednak jeśli program z jakiegoś powodu nie może utworzyć nowej kopii zapasowej, może dojść do sytuacji, w której nie będzie dostępna żadna kopia zapasowa.
Zastosuj reguły (tylko po skonfigurowaniu reguł przechowywania)	Określa, kiedy należy zastosować reguły przechowywania (s. 45). Procedurę czyszczenia można na przykład skonfigurować tak, aby była uruchamiana po każdym wykonaniu kopii zapasowej, a także według harmonogramu. Ta opcja jest dostępna tylko pod warunkiem, że w sekcji **Reguły przechowywania** została skonfigurowana przynajmniej jedna reguła przechowywania.
Harmonogram czyszczenia (tylko po wybraniu opcji **Według harmonogramu**)	Określa harmonogram procedury czyszczenia archiwum. Rozpoczęcie czyszczenia można na przykład zaplanować na ostatni dzień każdego miesiąca. Ta opcja jest dostępna tylko w przypadku wybrania parametru **Według harmonogramu** w sekcji **Zastosuj reguły**.

Przykłady

Tygodniowa pełna kopia zapasowa

Poniższy schemat umożliwia tworzenie pełnej kopii zapasowej w każdy piątek wieczorem.

Pełna kopia zapasowa: **Harmonogram: Co tydzień**, w każdy **piątek** o **22.00**

W tym przykładzie pola wszystkich parametrów z wyjątkiem **Harmonogram** w **Pełna kopia zapasowa** pozostają puste. Wszystkie kopie zapasowe w archiwum są przechowywane w nieskończoność (bez czyszczenia archiwów).

Pełna i przyrostowa kopia zapasowa plus czyszczenie

W następującym schemacie archiwum zawiera tygodniowe pełne i codzienne przyrostowe kopie zapasowe. Oprócz tego wymagamy również, aby program wykonał pełną kopię zapasową tylko po wylogowaniu wszystkich użytkowników.

Pełna kopia zapasowa: Harmonogram: Co tydzień, w każdy **Piątek** o **22.00**

Pełna kopia zapasowa: Warunki: Użytkownik wylogowany

Przyrostowa kopia zapasowa: Harmonogram: Co tydzień, w każdy dzień roboczy o **21.00**

Dodatkowo ustalamy usuwanie z archiwum kopii zapasowych starszych niż jeden rok oraz wykonywanie procedury czyszczenia po utworzeniu nowej kopii zapasowej.

Reguły przechowywania: Usuwaj kopie zapasowe starsze niż **12 miesięcy**

Zastosuj reguły: Po wykonaniu kopii zapasowej

Domyślnie jednoroczna pełna kopia zapasowa nie zostanie usunięta, dopóki wszystkie zależne od niej przyrostowe kopie zapasowe nie zostaną również usunięte. Więcej informacji znajduje się w sekcji Reguły przechowywania (s. 45).

Miesięczne pełne, tygodniowe różnicowe i dzienne przyrostowe kopie zapasowe plus czyszczenie

Ten przykład pokazuje zastosowanie wszystkich dostępnych opcji w schemacie niestandardowym.

Załóżmy, że chcemy stworzyć schemat, w ramach którego będą wykonywane miesięczne pełne kopie zapasowe, tygodniowe różnicowe kopie zapasowe i dzienne przyrostowe kopie zapasowe. Wówczas harmonogram tworzenia kopii zapasowych będzie wyglądał jak poniżej.

Pełna kopia zapasowa: Harmonogram: Co miesiąc, w każdą **ostatnią niedzielę** miesiąca o **21.00**

Przyrostowa kopia zapasowa: Harmonogram: Co tydzień, w każdy **dzień roboczy** o **19.00**

Różnicowa kopia zapasowa: Harmonogram: Co tydzień, w każdą **sobotę** o **20.00**

Oprócz tego chcemy dodać warunki, które muszą zostać spełnione, aby uruchomić zadanie tworzenia kopii zapasowej. Określa się je w polach **Warunki** dla każdego typu kopii zapasowej.

Pełna kopia zapasowa: **Warunki**: **Lokalizacja jest dostępna**

Przyrostowa kopia zapasowa: **Warunki**: **Użytkownik wylogowany**

Różnicowa kopia zapasowa: **Warunki**: **Użytkownik jest bezczynny**

Przy takich ustawieniach wykonanie pełnej kopii zapasowej — pierwotnie zaplanowanej na 21.00 — może faktycznie rozpocząć się później: gdy tylko będzie dostępna lokalizacja kopii zapasowej. Podobnie zadania tworzenia przyrostowych i różnicowych kopii zapasowych zostaną uruchomione dopiero, kiedy wszyscy użytkownicy odpowiednio wylogują się i będą bezczynni.

Na koniec tworzymy reguły przechowywania kopii w archiwum: zachowajmy tylko te kopie zapasowe, które nie są starsze niż sześć miesięcy i zezwólmy na wykonanie czyszczenia po każdym zadaniu tworzenia kopii zapasowej oraz również ostatniego dnia każdego miesiąca.

Reguły przechowywania: Usuwaj kopie zapasowe starsze niż **6 miesięcy**

Zastosuj reguły: **After backing up (Po utworzeniu kopii zapasowej)**, **Według harmonogramu**

Harmonogram czyszczenia: **Co miesiąc**, **Ostatni dzień**, **Wszystkie miesiące**, o **22.00**

Domyślnie program nie usuwa kopii zapasowej, dopóki istnieją zależne kopie zapasowe, które muszą zostać zachowane. Jeżeli na przykład pełna kopia zapasowa przeznaczona do usunięcia posiada zależne kopie przyrostowe lub różnicowe, usunięcie zostanie odłożone do momentu, kiedy będzie można usunąć również kopie zależne.

Więcej informacji znajduje się w części Reguły przechowywania (s. 45).

Zadania wynikowe

W każdym schemacie niestandardowym program zawsze generuje trzy zadania tworzenia kopii zapasowych oraz — jeśli określono reguły przechowywania — zadanie czyszczenia. Każde zadanie widnieje na liście zadań albo jako **Zaplanowane** (jeśli został skonfigurowany harmonogram), albo jako **Ręczne** (jeśli harmonogram nie został skonfigurowany).

Każde zadanie tworzenia kopii zapasowej lub zadanie czyszczenia można w dowolnym momencie uruchomić ręcznie — niezależnie od tego, czy znajduje się w harmonogramie.

W pierwszym z wcześniejszych przykładów skonfigurowany harmonogram przewidywał tworzenie tylko pełnych kopii zapasowych. Jednak schemat mimo to spowoduje powstanie trzech zadań, umożliwiając ręczne uruchomienie zadania tworzenia kopii zapasowej dowolnego typu:

- Tworzenie pełnej kopii zapasowej, uruchamiane w każdy piątek o 22:00
- Tworzenie przyrostowej kopii zapasowej, uruchamiane ręcznie
- Tworzenie różnicowej kopii zapasowej, uruchamiane ręcznie

Dowolne z tych zadań tworzenia kopii zapasowych można uruchomić, wybierając je z listy zadań w sekcji **Plany i zadania tworzenia kopii zapasowych** w lewym panelu.

Jeśli w schemacie tworzenia kopii zapasowych określono również reguły przechowywania, schemat spowoduje powstanie czterech zadań: trzech zadań tworzenia kopii zapasowych oraz jednego zadania czyszczenia.

7.3.8 Sprawdzanie poprawności archiwum

Należy skonfigurować zadanie sprawdzania poprawności, aby sprawdzić możliwość odzyskania danych z kopii zapasowych. Jeśli proces sprawdzania poprawności kopii zapasowej nie zakończy się pomyślnie, zadanie sprawdzania poprawności zakończy się niepowodzeniem, a plan tworzenia kopii zapasowych otrzyma status Błąd.

Aby skonfigurować sprawdzanie poprawności, określ następujące parametry

1. **Czas sprawdzania poprawności** — wybierz czas wykonywania zadania sprawdzania poprawności. Sprawdzanie poprawności to operacja intensywnie korzystająca z zasobów i zaleca się **zaplanowanie** sprawdzania poprawności na komputerze zarządzanym poza okresem największego ruchu. Jednak jeśli sprawdzanie poprawności stanowi zasadniczą część strategii ochrony danych i użytkownik chce niezwłocznie wiedzieć, czy dane kopii zapasowej są uszkodzone i czy można je pomyślnie odzyskać, warto rozważyć rozpoczęcie sprawdzania poprawności natychmiast po utworzeniu kopii zapasowej.
2. **Elementy do sprawdzenia poprawności** — wybierz sprawdzanie poprawności całego archiwum lub ostatniej kopii zapasowej w tym archiwum. Sprawdzanie poprawności kopii zapasowej plików symuluje odzyskiwanie wszystkich plików z kopii zapasowej do tymczasowego miejsca docelowego. Sprawdzanie poprawności kopii zapasowej woluminu polega na obliczeniu sumy kontrolnej wszystkich bloków danych zapisanych w kopii zapasowej. Sprawdzanie poprawności archiwum oznacza sprawdzenie poprawności wszystkich kopii zapasowych tego archiwum i może zająć dużo czasu oraz korzystać z dużej ilości zasobów systemu.
3. **Harmonogram sprawdzania poprawności** (pojawia się wyłącznie po wybraniu opcji Według harmonogramu w kroku 1) — określ harmonogram sprawdzania poprawności. Więcej informacji znajduje się w sekcji Tworzenie harmonogramu (s. 185).

8 Słownik

A

Acronis Active Restore

Technologia Acronis przywracająca połączenie internetowe niezwłocznie po rozpoczęciu odzyskiwania systemu. Komputer działa i udostępnia niezbędne usługi po uruchomieniu systemu z kopii zapasowej (s. 424). Najwyższy priorytet ma odzyskiwanie danych umożliwiających obsługę żądań przychodzących. Reszta danych jest odzyskiwana w tle. Ograniczenia:

- kopia zapasowa musi znajdować się na dysku lokalnym (dowolnym urządzeniu dostępnym z systemu BIOS, z wyjątkiem urządzenia uruchamianego przez sieć);
- nie działa z obrazami systemu Linux.

Acronis Plug-in for WinPE

Zmodyfikowana wersja komponentu Acronis Backup & Recovery 10 Agent for Windows, którą można uruchomić w środowisku przedinstalacyjnym. Wtyczkę można dodać do obrazu WinPE (s. 431) przy użyciu programu Generator nośnika startowego. Otrzymany nośnik startowy (s. 424) może służyć do uruchamiania dowolnego komputera klasy PC i umożliwia wykonywanie (z pewnymi ograniczeniami) większości operacji zarządzania bezpośredniego (s. 432) bez potrzeby korzystania z systemu operacyjnego. Operacje można konfigurować i nadzorować lokalnie za pośrednictwem graficznego interfejsu użytkownika lub zdalnie przy użyciu konsoli (s. 423).

Acronis Startup Recovery Manager (ASRM)

Zmodyfikowana wersja agenta startowego (s. 418), znajdująca się na dysku systemowym i uruchamiana po naciśnięciu klawisza F11 podczas uruchamiania komputera. Program Acronis Startup Recovery Manager eliminuje potrzebę użycia nośnika ratunkowego lub połączenia sieciowego w celu uruchomienia ratunkowego narzędzia startowego.

Acronis Startup Recovery Manager jest szczególnie przydatny dla użytkowników urządzeń przenośnych. W razie awarii należy ponownie uruchomić komputer, nacisnąć klawisz F11 po wyświetleniu monitu „Naciśnij klawisz F11, aby uruchomić Acronis Startup Recovery Manager…” oraz odzyskać dane w taki sam sposób jak ze zwykłego nośnika startowego.

Ograniczenie: wymaga ponownej aktywacji programów ładujących (nie dotyczy programu ładującego systemu Windows i GRUB).

Agent (Acronis Backup & Recovery 10 Agent)

Aplikacja do tworzenia kopii zapasowej danych i ich odzyskiwania oraz umożliwiająca wykonywanie innych operacji zarządzania na komputerze (s. 423), takich jak zarządzanie zadaniami i operacje na dysku twardym.

Typ danych, których kopię zapasową można utworzyć, zależy od typu agenta. Acronis Backup & Recovery 10 zawiera agenty do tworzenia kopii zapasowych dysków i plików oraz agenty do tworzenia kopii zapasowych maszyn wirtualnych znajdujących się na serwerach wirtualizacji.

Agent startowy

Ratunkowe narzędzie startowe z większością funkcji agenta Acronis Backup & Recovery 10 Agent (s. 418). Agent startowy korzysta z jądra systemu Linux. Komputer (s. 423) można uruchomić w agencie startowym przy użyciu nośnika startowego (s. 424) lub serwera Acronis PXE Server. Operacje można konfigurować i kontrolować lokalnie za pośrednictwem graficznego interfejsu użytkownika lub zdalnie przy użyciu konsoli (s. 423).

Archiwum

Zobacz Archiwum kopii zapasowej (s. 419).

Archiwum kopii zapasowej (Archiwum)

Zestaw kopii zapasowych (s. 424) tworzonych i zarządzanych według planu tworzenia kopii zapasowych (s. 425). W archiwum może znajdować się wiele pełnych kopii zapasowych (s. 425), jak również kopii przyrostowych (s. 426) i różnicowych (s. 427). Kopie zapasowe należące do tego samego archiwum są zawsze zachowywane w identycznej lokalizacji. Kopie zapasowe jednego źródła można tworzyć na podstawie wielu planów tworzenia kopii zapasowych i umieszczać w tym samym archiwum, ale podstawowy scenariusz to „jeden plan – jedno archiwum”.

Kopie zapasowe w archiwum są w całości zarządzane według planu tworzenia kopii zapasowych. Ręczne operacje na archiwach (sprawdzanie poprawności (s. 429), przeglądanie zawartości, montowanie i usuwanie kopii zapasowych) należy wykonywać przy użyciu produktu Acronis Backup & Recovery 10. Nie należy modyfikować archiwów przy użyciu narzędzi innych producentów niż Acronis, takich jak Eksplorator Windows lub menedżery plików innych firm.

Archiwum zaszyfrowane

Archiwum kopii zapasowej (s. 419) zaszyfrowane metodą AES (Advanced Encryption Standard). Jeśli w opcjach tworzenia kopii zapasowych (s. 425) są włączone szyfrowanie i hasło archiwum, każda kopia zapasowa należąca do archiwum przed zapisaniem w miejscu docelowym zostanie zaszyfrowana przez agenta (s. 418).

Algorytm kryptograficzny AES działa w trybie CBC (Cipher-block chaining) i korzysta z losowo wygenerowanego klucza o długości zdefiniowanej przez użytkownika: 128, 192 lub 256 bitów. Klucz szyfrowania jest następnie szyfrowany metodą AES-256 przy użyciu skrótu SHA-256 hasła jako klucza. Same hasło nie jest przechowywane w żadnej lokalizacji na dysku ani pliku kopii zapasowej. Skrót hasła służy do celów weryfikacji. Dzięki takim dwupoziomowym zabezpieczeniom dane kopii zapasowej są chronione przed nieautoryzowanym dostępem, ale odzyskanie utraconego hasła jest niemożliwe.

C

Czyszczenie

Usuwanie kopii zapasowych (s. 424) z archiwum kopii zapasowej (s. 419) w celu pozbycia się nieaktualnych kopii zapasowych lub zapobieżenia przekroczeniu żądanego rozmiaru archiwum.

Czyszczenie polega na zastosowaniu w archiwum reguł przechowywania, które zostały ustalone w planie tworzenia kopii zapasowych (s. 425) składających się na archiwum. Operacja powoduje sprawdzenie, czy nie został przekroczony maksymalny rozmiar archiwum i/lub czy istnieją

nieaktualne kopie zapasowe. W zależności od tego, czy zostały naruszone reguły przechowywania, operacja może, ale nie musi, prowadzić do usunięcia kopii zapasowych.

Aby uzyskać więcej informacji, zobacz Reguły przechowywania (s. 45).

Czyszczenie po stronie agenta

Czyszczenie (s. 419) wykonywane przez agenta (s. 418) zgodnie z planem tworzenia kopii zapasowych (s. 425), na podstawie którego powstało archiwum (s. 419). Czyszczenie po stronie agenta jest wykonywane w skarbcach niezarządzanych (s. 428).

Czyszczenie po stronie węzła magazynowania

Czyszczenie (s. 419) wykonywane w węźle magazynowania (s. 430) zgodnie z planami tworzenia kopii zapasowych (s. 425), w wyniku którego powstają archiwa (s. 419) przechowywane w skarbcu zarządzanym (s. 428). Będąc alternatywą dla czyszczenia po stronie agenta (s. 420), czyszczenie po stronie węzła magazynowania zmniejsza niepotrzebne obciążenie procesora w serwerach produkcyjnych.

Harmonogram czyszczenia istnieje na komputerze (s. 423), na którym znajduje się agent (s. 418), i dlatego korzysta z zegara i zdarzeń komputera. Agent musi zainicjować czyszczenie po stronie węzła magazynowania za każdym razem o zaplanowanej godzinie lub po wystąpieniu określonego zdarzenia. Aby było to możliwe, agent musi działać w trybie online.

W poniższej tabeli znajduje się zestawienie typów czyszczenia stosowanego w produkcie Acronis Backup & Recovery 10.

	Czyszczenie	
	Po stronie agenta	**Po stronie węzła magazynowania**
Dotyczy:	Archiwum	Archiwum
Inicjuje:	Agent	Agent
Wykonuje:	Agent	Węzeł magazynowania
Harmonogram ustalony przez:	Plan tworzenia kopii zapasowych	Plan tworzenia kopii zapasowych
Reguły przechowywania ustalone przez:	Plan tworzenia kopii zapasowych	Plan tworzenia kopii zapasowych

D

Deduplikacja

Metoda umożliwiająca zapis wielu duplikatów tej samej informacji tylko jeden raz.

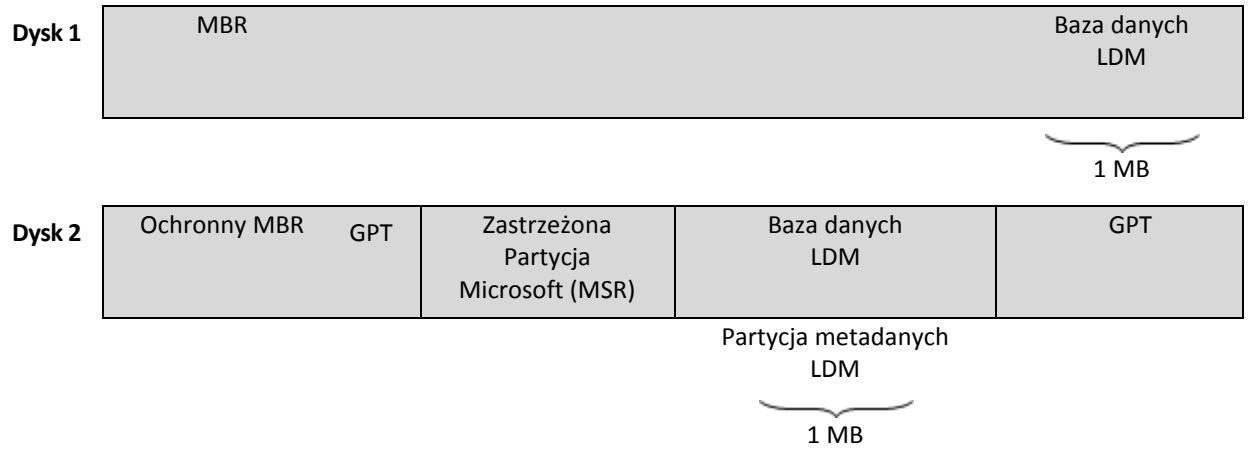
Produkt Acronis Backup & Recovery 10 umożliwia stosowanie technologii deduplikacji w archiwach kopii zapasowych (s. 419) przechowywanych w węzłach magazynowania (s. 430). Minimalizuje ona ilość miejsca zajmowanego przez archiwa oraz ruch sieciowy i wykorzystanie sieci podczas tworzenia kopii zapasowej.

Dysk dynamiczny

Dysk twardy zarządzany przez Menedżera dysków logicznych (LDM), który jest dostępny w systemach Windows, począwszy od Windows 2000. LDM ułatwia elastyczne przydzielanie woluminów na

urządzeniu pamięci w celu uzyskania wyższej odporności na uszkodzenia, wyższej wydajności lub większego rozmiaru woluminu.

Dysk dynamiczny może korzystać z głównego rekordu rozruchowego (MBR) lub stylu partycjonowania GPT z tabelą partycji GUID. Poza rekordem MBR lub stylem GPT na każdym dysku dynamicznych znajduje się ukryta baza danych, w której usługa LDM przechowuje informacje o konfiguracji woluminów dynamicznych. Na każdym dysku dynamicznym znajdują się pełne informacje o wszystkich woluminach dynamicznych istniejących w grupie dysków, co zapewnia większą niezawodność magazynu. Baza danych zajmuje przynajmniej 1 MB miejsca na dysku MBR. Na dysku GPT system Windows tworzy dedykowaną partycję metadanych usługi LDM, rezerwując dla niej miejsce na zastrzeżonej partycji firmy Microsoft (MSR).



Dyski dynamiczne są zorganizowane na dyskach MBR (dysk 1) i GPT (dysk 2).

Aby uzyskać więcej informacji na temat dysków dynamicznych, zobacz następujące artykuły bazy wiedzy Microsoft Knowledge Base:

Disk Management (Windows XP Professional Resource Kit) http://technet.microsoft.com/pl-pl/library/bb457110.aspx.

816307 Best practices for using dynamic disks on Windows Server 2003-based computers http://support.microsoft.com/kb/816307/pl.

Dziadek-ojciec-syn (GFS)

Popularny schemat tworzenia kopii zapasowych (s. 427) mający na celu zachowanie optymalnej proporcji między rozmiarem archiwum kopii zapasowej (s. 419) a liczbą punktów odzyskiwania (s. 426) dostępnych w archiwum. GFS umożliwia codzienne odzyskiwanie danych z ostatnich siedmiu dni, cotygodniowe — danych z ostatnich kilku tygodni oraz comiesięczne — danych z dowolnej chwili w przeszłości.

Aby uzyskać więcej informacji na ten temat, zobacz Schemat tworzenia kopii zapasowych dziadek-ojciec-syn (s. 38).

E

Eksportuj

Operacja, która tworzy kopię archiwum (s. 419) lub samowystarczalną częściową kopię archiwum w określonej lokalizacji. Operacja eksportu może być zastosowana do jednego archiwum, jednej kopii

zapasowej (s. 424) lub do wielu wybranych kopii należących do tego samego archiwum. Za pomocą interfejsu wiersza poleceń można wykonać eksport całego skarbca (s. 428).

G

Generator nośnika

Dedykowane narzędzie do tworzenia nośnika startowego (s. 424).

Grupa dynamiczna

Grupa komputerów (s. 423) wypełniana automatycznie przez serwer zarządzania (s. 427) zgodnie z kryteriami członkostwa, które zostały określone przez administratora. Produkt Acronis Backup & Recovery 10 oferuje następujące kryteria członkostwa:

- system operacyjny,
- jednostka organizacyjna usługi Active Directory,
- zakres adresów IP.

Komputer pozostaje w grupie dynamicznej dopóki spełnia kryteria członkostwa w grupie. Komputer zostanie z niej usunięty automatycznie, jeśli

- jego właściwości zmienią się w sposób uniemożliwiający dalsze spełniania kryteriów lub
- administrator zmieni kryteria w sposób uniemożliwiający ich dalsze spełnianie przez komputer.

Jedynym sposobem ręcznego usunięcia komputera z grupy dynamicznej jest usunięcie go z serwera zarządzania.

Grupa dysków

Określona liczba dysków dynamicznych (s. 420) do przechowywania typowych danych konfiguracyjnych w bazach danych LDM, którymi można zarządzać jako całością. Zwykle wszystkie dyski dynamiczne utworzone na tym samym komputerze (s. 423) należą do tej samej grupy dysków.

Po utworzeniu pierwszego dysku dynamicznego w LDM lub innym narzędziu do zarządzania dyskami nazwa grupy dysków pojawi się w kluczu rejestru HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\dmio\Boot Info\Primary Disk Group\Name.

Kolejne tworzone lub importowane dyski zostaną dodane do tej samej grupy dysków. Grupa istnieje dopóki istnieje przynajmniej jeden jej członek. Po odłączeniu ostatniego dysku dynamicznego lub skonwertowaniu go na dysk podstawowy grupa przestaje istnieć, ale jej nazwa pozostaje w kluczu rejestru podanym powyżej. Po ponownym utworzeniu lub podłączeniu dysku dynamicznego zostanie utworzona grupa dysków o nazwie przyrostowej.

Po przeniesieniu grupy dysków na inny komputer jest ona obsługiwana jako „obca” i nie można z niej korzystać dopóki nie zostanie zaimportowana do istniejącej grupy dysków. Import spowoduje aktualizację danych konfiguracyjnych zarówno na dyskach lokalnych, jak i obcych, dzięki czemu będą one tworzyć jedną grupę. Jeśli na komputerze nie istnieje żadna grupa dysków, grupa obca zostanie zaimportowana w aktualnej postaci (z oryginalną nazwą).

Aby uzyskać więcej informacji na temat grup dysków, zobacz następujący artykuł bazy wiedzy Microsoft Knowledge Base:

222189 Description of Disk Groups in Windows Disk Management
http://support.microsoft.com/kb/222189/pl-pl/.

Grupa statyczna

Grupa komputerów, które administrator serwera zarządzania (s. 427) wypełnia ręcznie, dodając je do grupy. Komputer pozostanie w grupie statycznej dopóki administrator nie usunie go z tej grupy lub z serwera zarządzania.

Grupa wbudowana

Grupa komputerów zawsze istniejąca na serwerze zarządzania (s. 427).

Na serwerze zarządzania istnieją dwie grupy wbudowane zawierające wszystkie komputery każdego typu: wszystkie komputery fizyczne (s. 423), wszystkie maszyny wirtualne (s. 424).

Grup wbudowanych nie można usunąć, przenieść do innych grup ani ręcznie zmodyfikować. W grupach wbudowanych nie można utworzyć grup niestandardowych. Jedynym sposobem usunięcia komputera fizycznego z grupy wbudowanej jest usunięcie tego komputera z serwera zarządzania. Maszyny wirtualne zostaną usunięte po usunięciu ich serwera hostów.

W grupie wbudowanej można zastosować zasady tworzenia kopii zapasowych (s. 433).

K

Komputer

Komputer fizyczny lub wirtualny o unikalnym identyfikatorze uzyskanym podczas instalacji systemu operacyjnego. Komputery z wieloma systemami operacyjnymi są obsługiwane jak wiele komputerów.

Komputer fizyczny

Na serwerze zarządzania Acronis Backup & Recovery 10 Management Server komputer fizyczny jest tożsamy z komputerem zarejestrowanym (s. 423). Maszyna wirtualna jest obsługiwana jak komputer fizyczny, jeśli został na niej zainstalowany agent Acronis Backup & Recovery 10, a maszyna została zarejestrowana na serwerze zarządzania.

Komputer zarejestrowany

Komputer (s. 423) zarządzany przez serwer zarządzania (s. 427). Komputer można zarejestrować tylko na jednym serwerze zarządzania naraz. Komputer zostanie zarejestrowany w wyniku wykonania procedury rejestracji (s. 427).

Komputer zarządzany

Komputer (s. 423) fizyczny lub wirtualny, na którym jest zainstalowany co najmniej jeden agent Acronis Backup & Recovery 10 (s. 418).

Konsola (Acronis Backup & Recovery 10 Management Console)

Narzędzie umożliwiające dostęp zdalny lub lokalny do agentów Acronis (s. 418) i serwera Acronis Backup & Recovery 10 Management Server (s. 427).

Po połączeniu konsoli z serwerem zarządzania administrator może ustalić zasady tworzenia kopii zapasowych (s. 433) i zarządzać nimi, a także uzyskać dostęp do innych funkcji serwera, co oznacza zarządzanie scentralizowane (s. 432). Korzystanie z bezpośredniego połączenia konsola-agent oznacza zarządzanie bezpośrednie (s. 432).

Konsolidacja

Scalenie dwóch lub więcej kolejnych kopii zapasowych (s. 424) z tego samego archiwum (s. 419) w jedną kopię zapasową.

Konsolidacja może być wymagana przy usuwaniu kopii zapasowych, zarówno ręcznym, jak i wykonywanym podczas czyszczenia (s. 419). Na przykład reguły przechowywania określają, że jest wymagane usunięcie nieaktualnej pełnej kopii zapasowej (s. 425), ale należy pozostawić kolejną kopię przyrostową (s. 426). Kopie zapasowe zostaną scalone w jedną pełną kopię zapasową, której datą utworzenia będzie data utworzenia przyrostowej kopii zapasowej. Konsolidacja może zająć dużo czasu i korzystać z dużej ilości zasobów, dlatego w regułach przechowywania istnieje opcja nieusuwania kopii zapasowych z zależnościami. W podanym przykładzie pełna kopia zapasowa będzie istnieć aż do czasu, gdy przyrostowa kopia zapasowa stanie się również nieaktualna. Wtedy obie kopie zapasowe zostaną usunięte.

Kopia zapasowa

Kopia zapasowa to wynik pojedynczej operacji tworzenia kopii zapasowej (s. 425). W ujęciu fizycznym jest to plik lub zapis na taśmie zawierający kopię zapasową danych wykonaną w określonym dniu o określonej godzinie. Pliki kopii zapasowych utworzone w programie Acronis Backup & Recovery 10 mają rozszerzenie TIB. Również pliki TIB powstałe w wyniku wyeksportowania (s. 421) lub konsolidacji (s. 424) kopii zapasowych są nazywane kopiami zapasowymi.

Kopia zapasowa (obraz) dysku

Kopia zapasowa (s. 424) „sektor po sektorze” dysku lub woluminu w postaci spakowanej. Zwykle są kopiowane tylko sektory zawierające dane. Produkt Acronis Backup & Recovery 10 udostępnia opcję utworzenia obrazu nieprzetworzonych danych, czyli skopiowania wszystkich sektorów dysku, dzięki czemu można uzyskać obraz nieobsługiwanych systemów plików.

L

Lokalny plan tworzenia kopii zapasowych

Plan tworzenia kopii zapasowych (s. 425) utworzony na komputerze zarządzanym (s. 423) przy użyciu zarządzania bezpośredniego (s. 432).

M

Maszyna wirtualna

Na serwerze zarządzania Acronis Backup & Recovery 10 Management Server maszyna (s. 423) jest obsługiwana jako wirtualna, jeśli można wykonać jej kopię zapasową z hosta wirtualizacji, nie instalując na niej agenta (s. 418). Maszyna wirtualna pojawia się na serwerze zarządzania po rejestracji serwera wirtualizacji obsługującego tę maszynę, pod warunkiem, że na serwerze jest zainstalowany agent Acronis Backup & Recovery 10 dla maszyn wirtualnych.

N

Nośnik startowy

Nośnik fizyczny (płyta CD, DVD lub flash USB albo inny nośnik obsługiwany jako urządzenie startowe w systemie BIOS komputera (s. 423)) zawierający agenta startowego (s. 418) lub Środowisko preinstalacyjne systemu Windows (WinPE) (s. 431) z wtyczką Acronis for WinPE (s. 418). Komputer można również uruchomić w tych środowiskach przy użyciu funkcji uruchamiania z sieci z serwera Acronis PXE Server lub serwera usługi instalacji zdalnej (RIS) firmy Microsoft. Takie serwery z przesłanymi komponentami startowymi można również uznać za rodzaj nośnika startowego.

Najczęstsze zastosowanie nośnika startowego:

- odzyskiwanie systemu operacyjnego, którego nie można uruchomić;
- uzyskanie dostępu do danych ocalałych w uszkodzonym systemie i utworzenie ich kopii zapasowej;
- wdrożenie systemu operacyjnego po awarii;
- utworzenie podstawowych lub dynamicznych woluminów (s. 431) po awarii;
- utworzenie kopii zapasowej „sektor po sektorze” dysku z nieobsługiwanym systemem plików;
- utworzenie w trybie offline kopii zapasowej wszelkich danych, których kopii zapasowej nie można utworzyć w trybie online ze względu na ograniczony dostęp, trwałą blokadę założoną przez uruchomione aplikacje lub z jakichkolwiek innych powodów.

O

Obraz

To samo, co kopia zapasowa dysku (s. 424).

Opcje tworzenia kopii zapasowych

Parametry konfiguracyjne operacji tworzenia kopii zapasowej (s. 425), takie jak polecenia poprzedzające tworzenie kopii zapasowej/następujące po nim, maksymalna przepustowość sieci przydzielona do strumienia kopii zapasowej lub poziom kompresji danych. Opcje tworzenia kopii zapasowych są częścią planu tworzenia kopii zapasowych (s. 425).

Operacja tworzenia kopii zapasowej

Operacja powodująca utworzenie kopii danych znajdujących się na dysku twardym komputera (s. 423) w celu odzyskania danych lub przywrócenia ich z określonego dnia i godziny.

P

Pełna kopia zapasowa

Samowystarczalna kopia zapasowa (s. 424) zawierająca wszystkie dane wybrane przy tworzeniu kopii zapasowej. Odzyskanie danych z pełnej kopii zapasowej nie wymaga dostępu do żadnej innej kopii zapasowej.

Plan

Zobacz Plan tworzenia kopii zapasowych (s. 425).

Plan tworzenia kopii zapasowych (Plan)

Zestaw reguł określających sposób ochrony konkretnych danych na danym komputerze. Elementy określone w planie tworzenia kopii zapasowych:

- dane uwzględniane w kopii zapasowej;
- miejsce przechowywania archiwum kopii zapasowej (s. 419) (nazwa i lokalizacja archiwum kopii zapasowej);
- schemat tworzenia kopii zapasowych (s. 427) zawierający harmonogram tworzenia kopii zapasowych i (opcjonalnie) reguły ich przechowywania;
- reguły sprawdzania poprawności (s. 426) archiwum (opcjonalnie);
- opcje tworzenia kopii zapasowych(opcjonalnie) (s. 425).

Na przykład w planie tworzenia kopii zapasowych mogą się znajdować następujące informacje:

- utwórz kopię zapasową woluminu C: **(są to dane objęte planową ochroną)**;
- nadaj archiwum nazwę MySystemVolume i umieść je w lokalizacji \\server\backups\ **(są to nazwa i lokalizacja archiwum kopii zapasowej)**;
- utwórz pełną kopię zapasową co miesiąc w ostatni dzień miesiąca o godzinie 10.00 oraz przyrostową kopię zapasową w każdą niedzielę o godzinie 22.00. Usuń kopie zapasowe starsze niż 3 miesiące **(jest to schemat tworzenia kopii zapasowych)**;
- sprawdź poprawność ostatniej kopii zapasowej niezwłocznie po jej utworzeniu **(jest to reguła sprawdzania poprawności)**;
- chroń archiwum hasłem **(jest to opcja)**.

Fizycznie plan tworzenia kopii zapasowych to pakiet zadań (s. 431) przeznaczonych do wykonania na komputerze zarządzanym (s. 423).

Plan tworzenia kopii zapasowych można utworzyć bezpośrednio na komputerze (plan lokalny) lub może się on pojawić na komputerze w wyniku wdrożenia zasad tworzenia kopii zapasowych (s. 433) (plan scentralizowany (s. 427)).

Przyrostowa kopia zapasowa

Kopia zapasowa (s. 424) do przechowywania danych, które zostały zmienione od czasu tworzenia ostatniej kopii zapasowej. Aby odzyskać dane z przyrostowej kopii zapasowej, należy uzyskać dostęp do innych kopii zapasowych z tego samego archiwum (s. 419).

Punkt odzyskiwania

Data i godzina utworzenia kopii zapasowej danych, które można przywrócić.

R

Reguła wyboru

Część zasad tworzenia kopii zapasowych (s. 433). Umożliwia administratorowi serwera zarządzania (s. 427) wybór danych na komputerze, dla których ma zostać utworzona kopia zapasowa.

Reguły sprawdzania poprawności

Część planu tworzenia kopii zapasowych (s. 425). Reguły definiują czas i częstotliwość operacji sprawdzania poprawności (s. 429). Definiują również, czy ma być sprawdzana poprawność całego archiwum (s. 419) czy ostatniej kopii zapasowej w tym archiwum.

Rejestracja

Procedura umożliwiająca dodanie komputera zarządzanego (s. 423) do serwera zarządzania (s. 427).

Rejestracja polega na utworzeniu relacji zaufania między agentami (s. 418) znajdującymi się na komputerze i serwerze. Podczas rejestracji konsola pobiera certyfikat kliencki serwera zarządzania i przekazuje go do agenta, który użyje go później do uwierzytelnienia klientów nawiązujących połączenie. Dzięki temu można zapobiec wszelkim próbom ataków sieciowych polegających na ustanowieniu fałszywego połączenia w imieniu zaufanego podmiotu zabezpieczeń (serwera zarządzania).

Różnicowa kopia zapasowa

W różnicowej kopii zapasowej są zapisywane dane, które zostały zmienione od czasu utworzenia ostatniej pełnej kopii zapasowej (s. 425). Aby odzyskać dane z różnicowej kopii zapasowej, należy uzyskać dostęp do odpowiedniej pełnej kopii zapasowej.

S

Scentralizowany plan tworzenia kopii zapasowych

Plan tworzenia kopii zapasowych (s. 425) pojawiający się na komputerze zarządzanym (s. 423) w wyniku wdrożenia zasad tworzenia kopii zapasowych (s. 433) z serwera zarządzania (s. 427). Taki plan można zmodyfikować tylko przez edycję zasad tworzenia kopii zapasowych.

Schemat tworzenia kopii zapasowych

Część planu tworzenia kopii zapasowych (s. 425) obejmująca harmonogram tworzenia kopii zapasowych oraz (opcjonalnie) reguły przechowywania i harmonogram czyszczenia (s. 419). Na przykład: twórz pełną kopię zapasową (s. 425) co miesiąc w ostatni dzień miesiąca o godzinie 10:00 oraz przyrostową kopię zapasową (s. 426) w każdą niedzielę o godzinie 22:00. Usuń kopie zapasowe starsze niż 3 miesiące. Sprawdź obecność takich kopii po ukończeniu każdej operacji tworzenia kopii zapasowej.

Program Acronis Backup & Recovery 10 udostępnia dobrze znane, zoptymalizowane schematy tworzenia kopii zapasowych, takie jak GFS i Wieża Hanoi, przy użyciu których można opracowywać własne schematy tworzenia kopii zapasowych lub jednorazowo tworzyć kopie zapasowe danych.

Serwer zarządzania (Acronis Backup & Recovery 10 Management Server)

Serwer centralny zapewniający ochronę danych w sieci przedsiębiorstwa. Acronis Backup & Recovery 10 Management Server to dla administratora:

- jeden punkt wejścia do infrastruktury Acronis Backup & Recovery 10;
- łatwy sposób ochrony danych na licznych komputerach (s. 423) przy użyciu zasad tworzenia kopii zapasowych (s. 433) i grupowania;
- funkcja monitorowania całego przedsiębiorstwa;

- opcja tworzenia skarbców centralnych (s. 428) do przechowywania archiwów kopii zapasowych (s. 419) przedsiębiorstwa;
- opcja zarządzania węzłami magazynowania (s. 430).

Jeśli w sieci istnieje wiele serwerów zarządzania, działają one niezależnie, zarządzają innymi komputerami i korzystają z innych skarbców centralnych do przechowywania archiwów.

Skarbiec

Miejsce do zachowywania archiwów kopii zapasowych (s. 419). Skarbiec można zorganizować na dysku lokalnym lub sieciowym albo nośniku wymiennym, takim jak zewnętrzny dysk USB. Nie istnieją ustawienia umożliwiające ograniczenie rozmiaru skarbca ani liczby kopii zapasowych w skarbcu. Rozmiar każdego archiwum można ograniczyć, korzystając z funkcji czyszczenia (s. 419), ale całkowity rozmiar archiwów przechowywanych w skarbcu jest ograniczony tylko rozmiarem magazynu.

Skarbiec centralny

Lokalizacja sieciowa wyznaczona przez administratora serwera zarządzania (s. 427) do przechowywania archiwów kopii zapasowych (s. 419). Skarbiec centralny może być zarządzany przy użyciu węzła magazynowania (s. 430) albo niezarządzany. Łączna liczba archiwów przechowywanych w skarbcu centralnym i ich rozmiar są ograniczone wyłącznie rozmiarem magazynu.

Niezwłocznie po utworzeniu skarbca centralnego przez administratora serwera zarządzania nazwa i ścieżka tego skarbca są dystrybuowane na wszystkie komputery zarejestrowane (s. 423) na serwerze. Na liście skarbców centralnych dostępnej na komputerach pojawi się skrót do skarbca. Ze skarbca centralnego można korzystać we wszelkich planach tworzenia kopii zapasowych (s. 425) istniejących na komputerach, w tym również planach lokalnych.

Na komputerze, który nie jest zarejestrowany na serwerze zarządzania, użytkownik mający uprawnienia do tworzenia kopii zapasowej w skarbcu centralnym może wykonać tę czynność, określając pełną ścieżkę do skarbca. Jeśli skarbiec jest zarządzany, przy użyciu węzła magazynowania zarządzane będą zarówno archiwa użytkownika, jak i inne archiwa przechowywane w skarbcu.

Skarbiec deduplikacji

Skarbiec zarządzany (s. 428), w którym można wykonać deduplikację (s. 420).

Skarbiec niezarządzany

Każdy skarbiec (s. 428), który nie jest skarbcem zarządzanym (s. 428).

Skarbiec osobisty

Skarbiec (s. 428) lokalny lub sieciowy utworzony przy użyciu funkcji zarządzania bezpośredniego (s. 432). Po utworzeniu skarbca osobistego skrót do niego pojawi się w elemencie **Skarbce osobiste** panelu **Nawigacja**. Ze skarbca osobistego znajdującego się w określonej lokalizacji fizycznej, takiej jak udział sieciowy, może korzystać wiele komputerów.

Skarbiec zarządzany

Skarbiec centralny (s. 428) zarządzany w węźle magazynowania (s. 430). Dostęp do archiwów (s. 419) w skarbcu zarządzanym można uzyskać w następujący sposób:

bsp://adres_węzła/nazwa_skarbca/nazwa_archiwum/

Fizycznie skarbce zarządzane mogą znajdować się w udziale sieciowym, SAN, NAS, na dysku twardym lokalnym dla węzła magazynowania lub w bibliotece taśm podłączonej lokalnie do węzła magazynowania. W węźle magazynowania jest wykonywane czyszczenie po stronie węzła magazynowania (s. 420) i sprawdzanie poprawności po stronie węzła magazynowania (s. 429) dla każdego archiwum przechowywanego w skarbcu zarządzanym. Administrator może określić dodatkowe operacje, które będą wykonywane w węźle magazynowania (deduplikacja (s. 420), szyfrowanie).

Każdy skarbiec zarządzany jest niezależny, co oznacza, że zawiera wszystkie metadane potrzebne do zarządzania nim w węźle magazynowania. W razie utraty węzła magazynowania lub uszkodzenia jego bazy danych nowy węzeł magazynowania pobierze metadane i ponownie utworzy bazę danych. Ta sama procedura zostanie wykonana po podłączeniu skarbca do innego węzła magazynowania.

Skarbiec zaszyfrowany

Skarbiec zarządzany (s. 428), w którym wszystkie zapisywane dane są szyfrowane, a wszystkie odczytywane dane są deszyfrowane w czasie rzeczywistym przez węzeł magazynowania (s. 430) przy użyciu klucza szyfrowania skarbca przechowywanego w tym węźle. W przypadku kradzieży nośnika magazynu lub uzyskania do niego dostępu przez osobę nieautoryzowaną odszyfrowanie zawartości skarbca bez dostępu do węzła magazynowania będzie niemożliwe. Archiwa zaszyfrowane (s. 419) będą szyfrowane przez agenta (s. 418).

Sprawdzanie poprawności

Operacja sprawdzająca, czy można odzyskać dane z kopii zapasowej (s. 424).

Sprawdzanie poprawności kopii zapasowej plików symuluje odzyskiwanie wszystkich plików z kopii zapasowej do tymczasowego miejsca docelowego. W starszych wersjach produktu kopia zapasowa plików była prawidłowa, jeśli w jej nagłówku znajdowały się spójne metadane. Obecna metoda zajmuje więcej czasu, ale jest bardziej niezawodna. Sprawdzanie poprawności kopii zapasowej woluminu polega na obliczeniu sumy kontrolnej wszystkich bloków danych zapisanych w kopii zapasowej. Jest to również procedura intensywnie korzystająca z zasobów.

Operacja sprawdzania poprawności zakończona powodzeniem oznacza wysokie prawdopodobieństwo pomyślnego odzyskania danych. Nie są jednak sprawdzane wszystkie czynniki, które mają wpływ na proces odzyskiwania. Po utworzeniu kopii zapasowej systemu operacyjnego gwarancję pomyślnego odzyskania danych w przyszłości można uzyskać jedynie na podstawie testu, który polega na odzyskaniu danych z nośnika startowego na zapasowy dysk twardy.

Sprawdzanie poprawności po stronie agenta

Sprawdzanie poprawności (s. 429) wykonywane przez agenta (s. 418) zgodnie z planem tworzenia kopii zapasowych (s. 425), na podstawie którego powstało archiwum (s. 419). Sprawdzanie poprawności po stronie agenta jest wykonywane w skarbcach niezarządzanych (s. 428).

Sprawdzanie poprawności po stronie węzła magazynowania

Sprawdzanie poprawności (s. 429) wykonywane w węźle magazynowania (s. 430) zgodnie z planami tworzenia kopii zapasowych (s. 425), w wyniku którego powstają archiwa (s. 419) przechowywane w lokalizacji zarządzanej (s. 428). Będąc alternatywą dla sprawdzania poprawności po stronie agenta (s.

429), sprawdzanie poprawności po stronie węzła magazynowania zmniejsza niepotrzebne obciążenie procesora w serwerach produkcyjnych.

Strefa Acronis Secure Zone

Bezpieczny wolumin do przechowywania archiwów (s. 419) kopii zapasowych na komputerze zarządzanym (s. 423). Zalety:

- umożliwia odzyskanie zawartości dysku na ten sam dysk, na którym znajduje się jego kopia zapasowa;
- tania i przydatna metoda ochrona danych przed nieprawidłowym działaniem oprogramowania, atakiem wirusów, błędem operatora;
- eliminuje potrzebę użycia dodatkowego nośnika lub połączenia sieciowego w celu utworzenia kopii zapasowej lub odzyskania danych. Jest to szczególnie przydatne dla użytkowników urządzeń mobilnych;
- może służyć jako lokalizacja podstawowa dla kopii zapasowej w podwójnej lokalizacji.

Ograniczenia: Strefy Acronis Secure Zone nie można utworzyć na dysku dynamicznym (s. 420) ani na dysku, na którym stosowany jest styl partycjonowania GPT.

Strefa Acronis Secure Zone jest obsługiwana jako skarbiec osobisty (s. 428).

U

Universal Restore (Acronis Backup & Recovery 10 Universal Restore)

Zastrzeżona technologia firmy Acronis, która ułatwia uruchamianie systemu Windows na sprzęcie o innej konfiguracji lub na maszynie wirtualnej. Moduł Universal Restore niweluje różnice między urządzeniami istotnymi dla uruchamiania systemu operacyjnego, takimi jak kontrolery pamięci, płyta główna i chipset.

Moduł Universal Restore jest niedostępny w następujących przypadkach:

- uruchamianie komputera za pomocą programu Acronis Startup Recovery Manager (s. 418) (przez naciśnięcie klawisza F11),
- umiejscowienie odzyskiwanego obrazu w strefie Acronis Secure Zone (s. 430),
- używanie funkcji Acronis Active Restore (s. 418),

ponieważ są to funkcje przeznaczone głównie do natychmiastowego odzyskiwania danych na tym samym komputerze.

Moduł Universal Restore jest niedostępny w przypadku odzyskiwania systemu Linux.

W

Węzeł magazynowania (Acronis Backup & Recovery 10 Storage Node)

Serwer mający na celu optymalizację wykorzystania różnych zasobów wymaganych do ochrony danych przedsiębiorstwa. Cel ten jest uzyskiwany dzięki organizacji skarbców zarządzanych (s. 428). Węzeł magazynowania umożliwia administratorowi:

- zmniejszenie niepotrzebnego obciążenia procesora na komputerach zarządzanych (s. 423) przy użyciu czyszczenia po stronie węzła magazynowania (s. 420) i sprawdzania poprawności po stronie węzła magazynowania (s. 429);

- znaczące zmniejszenie ruchu dotyczącego kopii zapasowej oraz ilości miejsca zajmowanego w magazynie przez archiwa (s. 419) dzięki użyciu deduplikacji (s. 420);
- zapobieżenie dostępowi do archiwów kopii zapasowych nawet w przypadku kradzieży nośnika magazynu lub uzyskaniu dostępu przez osobę nieautoryzowaną — dzięki użyciu skarbców zaszyfrowanych (s. 429).

Wieża Hanoi

Popularny schemat tworzenia kopii zapasowych (s. 427) mający na celu zachowanie optymalnej proporcji między rozmiarem archiwum kopii zapasowej (s. 419) a liczbą punktów odzyskiwania (s. 426) dostępnych w archiwum. W odróżnieniu od schematu dziadek-ojciec-syn (s. 421) mającego tylko trzy poziomy odzyskiwania (codziennie, co tydzień, co miesiąc), schemat Wieża Hanoi wraz ze zwiększaniem się wieku kopii zapasowej stale zmniejsza interwał czasu między kolejnymi punktami odzyskiwania. Dzięki temu można bardzo efektywnie korzystać z magazynu kopii zapasowych.

Aby uzyskać więcej informacji na ten temat, zobacz „Schemat tworzenia kopii zapasowych — Wieża Hanoi (s. 42)”.

WinPE (Środowisko preinstalacyjne systemu Windows)

Minimalna wersja systemu Windows wykorzystująca jedno z następujących jąder:

- Windows XP Professional z dodatkiem Service Pack 2 (PE 1.5);
- Windows Server 2003 z dodatkiem Service Pack 1 (PE 1.6);
- Windows Vista (PE 2.0);
- Windows Vista z dodatkiem SP1 i Windows Server 2008 (PE 2.1).

WinPE jest zwykle używane przez producentów OEM i firmy w celu wdrożenia, przetestowania, zdiagnozowania i naprawy systemu. Komputer z systemem WinPE można uruchomić z serwera PXE, płyty CD-ROM, dysku USB flash lub dysku twardego. Wtyczka Acronis Plug-in for WinPE (s. 418) umożliwia uruchomienie agenta Acronis Backup & Recovery 10 (s. 418) w środowisku przedinstalacyjnym.

Wolumin dynamiczny

Dowolny wolumin znajdujący się na dyskach dynamicznych (s. 420), a dokładniej — w grupie dysków (s. 422). Woluminy dynamiczne mogą zajmować wiele dysków i są zwykle skonfigurowane w zależności od celu ich utworzenia:

- zwiększenie rozmiaru woluminu (wolumin łączony);
- skrócenie czasu dostępu (wolumin rozłożony);
- uzyskanie odporności na uszkodzenia przez wprowadzenie nadmiarowości (woluminy lustrzane i RAID-5).

Z

Zadanie

W programie Acronis Backup & Recovery 10 jest to zestaw kolejnych czynności do wykonania na komputerze zarządzanym (s. 423) w określonym czasie lub po wystąpieniu określonego zdarzenia. Czynności są opisane w pliku skryptowym xml. Warunek początkowy (harmonogram) jest określony w chronionych kluczach rejestru.

Zadanie lokalne

Zadanie (s. 431) należące do lokalnego planu tworzenia kopii zapasowych (s. 424) lub zadanie nienależące do żadnego planu, takie jak zadania odzyskania. Zadanie lokalne należące do planu tworzenia kopii zapasowych można zmodyfikować tylko przez edycję planu. Inne zadania lokalne można zmodyfikować bezpośrednio.

Zadanie scentralizowane

Zadanie (s. 431) należące do scentralizowanego planu tworzenia kopii zapasowych (s. 427). Zadanie takie pojawia się na komputerze zarządzanym (s. 423) w wyniku wdrożenia zasad tworzenia kopii zapasowych (s. 433) z serwera zarządzania (s. 427) i można je zmodyfikować tylko przez edycję zasad tworzenia kopii zapasowych.

Zarządzanie bezpośrednie

Dowolna operacja zarządzania wykonywana na komputerze zarządzanym (s. 423) przy użyciu bezpośredniego połączenia konsola (s. 423)-agent (s. 418) (w przeciwieństwie do zarządzania scentralizowanego (s. 432), w którym operacje są konfigurowane na serwerze zarządzania (s. 427) i propagowane przez serwera na komputery zarządzane).

Operacje zarządzania bezpośredniego:

- tworzenie lokalnych planów tworzenia kopii zapasowych (s. 424) i zarządzanie nimi;
- tworzenie zadań lokalnych (s. 431), takich jak zadania odzyskiwania, i zarządzanie nimi;
- tworzenie skarbców osobistych (s. 428) i archiwów tam przechowywanych oraz zarządzanie nimi;
- wyświetlanie stanu, postępu i właściwości zadań scentralizowanych (s. 432) istniejących na komputerze;
- przeglądanie dziennika operacji agenta i zarządzanie nim;
- operacje zarządzania dyskami, takie jak klonowanie dysku oraz tworzenie i konwertowanie woluminu.

Rodzaj zarządzania bezpośredniego przy użyciu nośnika startowego (s. 424). Niektóre operacje zarządzania bezpośredniego można również wykonać za pośrednictwem graficznego interfejsu użytkownika serwera zarządzania. Jednak taki scenariusz zakłada jawne lub ukryte połączenie bezpośrednie z wybranym komputerem.

Zarządzanie scentralizowane

Zarządzanie infrastrukturą Acronis Backup & Recovery 10 za pośrednictwem jednostki zarządzania centralnego jest znane jako serwer zarządzania Acronis Backup & Recovery 10 (s. 427). Do operacji zarządzania scentralizowanego zalicza się:

- tworzenie i stosowanie zasad tworzenia kopii zapasowych (s. 433) oraz zarządzanie nimi;
- tworzenie statycznych (s. 423) i dynamicznych grup (s. 422) komputerów (s. 423) oraz zarządzanie nimi;
- zarządzanie zadaniami (s. 431) istniejącymi na komputerach;
- tworzenie skarbców centralnych (s. 428) do przechowywania archiwów i zarządzanie nimi;
- zarządzanie węzłami magazynowania (s. 430);
- monitorowanie działania komponentów produktu Acronis Backup & Recovery 10, przeglądanie dzienników scentralizowanych itd.

Zasady

Zobacz Zasady tworzenia kopii zapasowych (s. 433).

Zasady tworzenia kopii zapasowych (Zasady)

Szablon planu tworzenia kopii zapasowych utworzony przez administratora serwera zarządzania (s. 427) i zapisany na tym serwerze. Zasady tworzenia kopii zapasowych zawierają te same reguły, co plan tworzenia kopii zapasowych, ale mogą nie określać wprost elementów danych, dla których ma być utworzona kopia zapasowa. W zamian można zastosować reguły wyboru (s. 426), takie jak zmienne środowiskowe. Ze względu na taką elastyczność zasady tworzenia kopii zapasowych można zastosować centralnie na wielu komputerach. Jeśli element danych jest określony wprost (np. /dev/sda lub C:\Windows), zasady spowodują utworzenie kopii zapasowej tego elementu na każdym komputerze, na którym zostanie znaleziona dokładnie ta ścieżka.

Stosując zasady w grupie komputerów, administrator może wdrożyć wiele planów tworzenia kopii zapasowych przez wykonanie jednej czynności.

Przepływ pracy przy stosowaniu zasad jest następujący.

1. Administrator tworzy zasady tworzenia kopii zapasowych.
2. Administrator stosuje zasady w grupie komputerów lub na pojedynczym komputerze (s. 423).
3. Serwer zarządzania wdraża zasady na komputerach.
4. Na każdym komputerze zainstalowany agent (s. 418) znajduje elementy danych na podstawie reguł wyboru. Na przykład jeśli reguła wyboru to [Wszystkie woluminy], zostanie utworzona kopia zapasowa całego systemu.
5. Na każdym komputerze zainstalowany agent tworzy plan tworzenia kopii zapasowych (s. 425) na podstawie innych reguł, które zostały określone w zasadach. Taki plan tworzenia kopii zapasowych to plan scentralizowany (s. 427).
6. Na każdym komputerze zainstalowany agent tworzy zestaw zadań scentralizowanych (s. 432), które będą wykonywane według planu.