Acronis

Acronis Backup 12

Update 3

PODRĘCZNIK UŻYTKOWNIKA

Spis treści

Copyright © Acronis International GmbH, 2002-2017

Copyright © Acronis International GmbH, 2002-2017

Copyright © Acronis International GmbH, 2002-2017

Copyright © Acronis International GmbH, 2002-2017

1 Co nowego w programie Acronis Backup

1.1 Co nowego w wersji Update 3

- Tworzenie kopii zapasowych i odzyskiwanie skrzynek pocztowych Office 365 (s. 121)
- Możliwość tworzenia i usuwania strefy Secure Zone w interfejsie internetowym (s. 48)
- Obsługa środowisk vSphere 6.5, Red Hat Enterprise Virtualization 3.6 i 4.0, Microsoft Hyper-V Server 2016 (s. 14)
- Obsługa wersji 4.7–4.9 jądra systemu Linux
- Obsługa systemów Red Hat Enterprise Linux 7.3, Oracle Linux 7.3, CentOS 7.2 i 7.3, Debian 8.4 i 8.5

1.2 Co nowego w wersji Update 2

- Obsługa systemu macOS Sierra 10.12

1.3 Co nowego w programie Acronis Backup 12

- Zupełnie nowy, nowocześnie wyglądający interfejs internetowy (s. 39)
- Serwer zarządzania — centralny punkt zarządzania wszystkimi kopiami zapasowymi

Instalacja

- Wdrożenie chmurowe lub lokalne (s. 7)
- Zdalna instalacja agentów (s. 24)

Kopia zapasowa aplikacji

- Tworzenie kopii zapasowych baz danych programu Exchange (s. 111)
- Tworzenie kopii zapasowych baz danych SQL (s. 110)
- Tworzenie uwzględniających aplikacje kopii zapasowych komputerów fizycznych i maszyn wirtualnych (s. 112)
- Odzyskiwanie granularne danych programu Exchange (s. 117)

Wirtualizacja

- Tworzenie kopii zapasowych maszyn wirtualnych Hyper-V
- Uruchamianie maszyny wirtualnej z kopii zapasowej (Instant Restore) (s. 123)
- Replikacja maszyn wirtualnych ESXi (s. 126)
- Optymalizacja sieci WAN pod kątem replikacji maszyn wirtualnych (seeding replik) (s. 130) — tylko we wdrożeniach lokalnych
- Odzyskiwanie plików na maszyny wirtualne ESXi (s. 82)
- Odzyskiwanie maszyn ESXi na komputer bez systemu operacyjnego (s. 46)
- Agentowe tworzenie kopii zapasowych maszyn wirtualnych znajdujących się w środowiskach Windows Azure i Amazon EC2 (s. 138)
- Technologia Flashback — przyrostowe odzyskiwanie maszyn wirtualnych (s. 89)

Funkcje ogólne

- Tworzenie kopii zapasowych systemów Mac

Copyright © Acronis International GmbH, 2002-2017

- Tworzenie kopii zapasowych urządzeń mobilnych (s. 103) — tylko we wdrożeniach chmurowych
- Zarządzanie grupami i kontami (s. 140) — tylko we wdrożeniach chmurowych
- Wyszukiwanie plików i folderów w kopii zapasowej (s. 82)
- Zaawansowane filtry plików (s. 60)

2 Instalacja

2.1 Omówienie instalacji

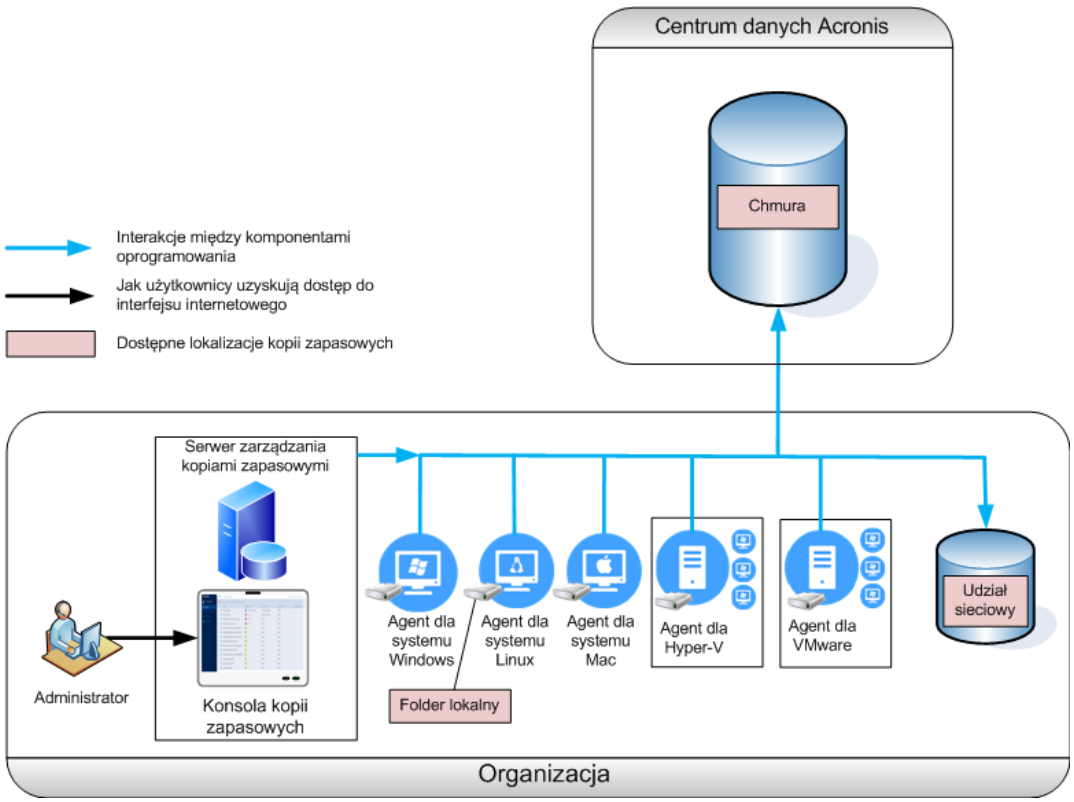
Program Acronis Backup obsługuje dwie metody wdrożenia: lokalnie oraz w chmurze. Metody te różnią się przede wszystkim lokalizacją komponentu Acronis Backup Management Server.

Acronis Backup Management Server jest centralnym punktem zarządzania wszystkimi kopiami zapasowymi. W przypadku wdrożenia lokalnego jest on instalowany w sieci lokalnej. W przypadku wdrożenia chmurowego znajduje się w jednym z centrów danych Acronis. Interfejs internetowy tego serwera jest nazywany konsolą kopii zapasowych.

Oba rodzaje wdrożeń wymagają instalacji agenta kopii zapasowych na każdym komputerze, którego kopię zapasową chcesz utworzyć. Obsługiwane są też takie same typy magazynów: foldery lokalne, udziały sieciowe oraz chmura Acronis Cloud Storage. Miejsce w chmurze jest sprzedawane oddzielnie od licencji programu Acronis Backup.

Wdrożenie lokalne

Wdrożenie lokalne oznacza, że wszystkie komponenty produktu są instalowane w sieci lokalnej. Jest to jedyna metoda wdrożenia dostępna z licencją wieczystą. Z metody tej trzeba skorzystać również wtedy, gdy komputery nie są podłączone do Internetu.



Copyright © Acronis International GmbH, 2002-2017

Lokalizacja serwera zarządzania

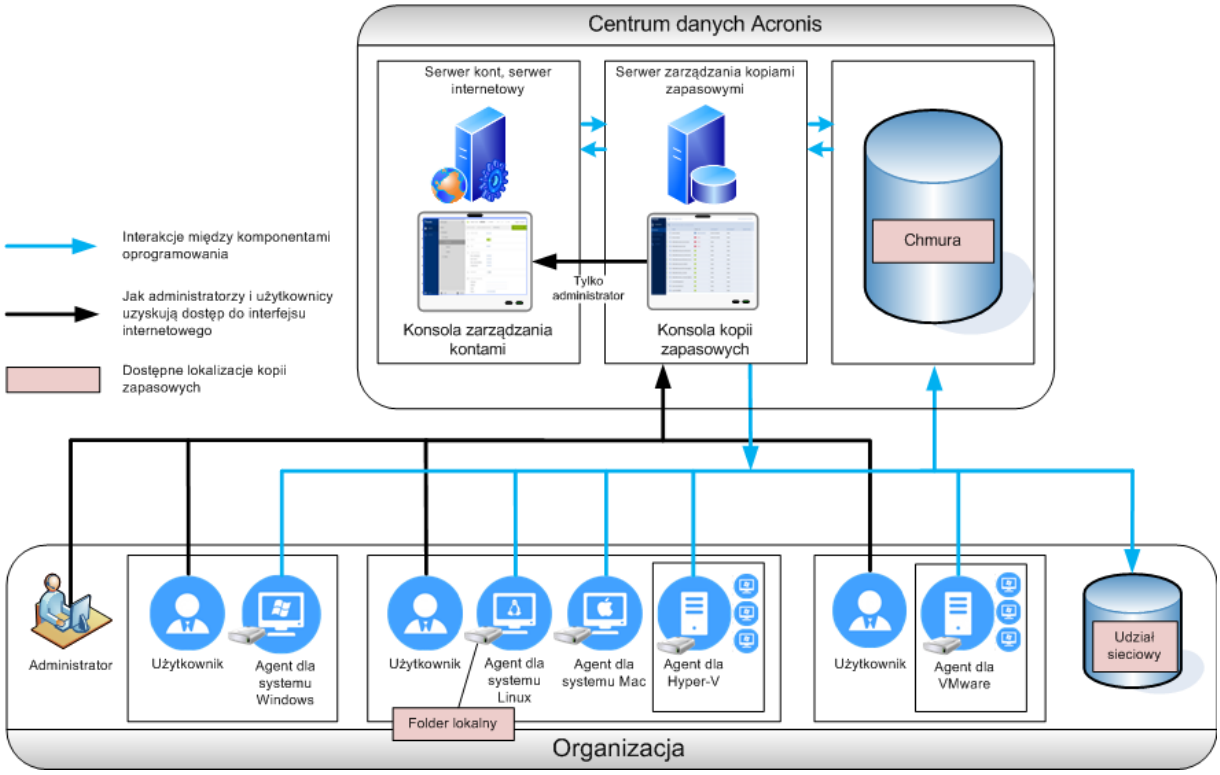
Serwer zarządzania można zainstalować na komputerze z systemem Windows lub Linux. Zalecana jest instalacja w systemie Windows, ponieważ umożliwia ona wdrażanie agentów na innych komputerach z poziomu serwera zarządzania. Instalacja w systemie Linux jest zalecana w środowiskach opartych wyłącznie na systemie Linux. Agenta trzeba zainstalować lokalnie na komputerach, których kopie zapasowe chcesz utworzyć.

Wdrożenie chmurowe

Wdrożenie chmurowe oznacza, że serwer zarządzania znajduje się w jednym z centrów danych Acronis. Zaletą tego rozwiązania jest brak konieczności konserwacji serwera zarządzania w sieci lokalnej. Program Acronis Backup można w tym przypadku uznać za usługę tworzenia kopii zapasowych świadczoną przez firmę Acronis.

Dostęp do serwera kont umożliwia tworzenie kont użytkowników, ustawianie dla nich limitów korzystania z usług oraz tworzenie grup użytkowników (jednostek) odzwierciedlających strukturę organizacji. Każdy użytkownik może uzyskać dostęp do konsoli kopii zapasowych, pobrać wymaganego agenta i w kilka minut zainstalować go na swoich komputerach.

Konta administratorów można tworzyć na poziomie jednostki lub organizacji. Każde konto ma widok swojego obszaru kontroli. Użytkownicy mają dostęp tylko do własnych kopii zapasowych.



W poniższej tabeli zestawiono różnice między wdrożeniem lokalnym a wdrożeniem chmurowym.

Copyright © Acronis International GmbH, 2002-2017

Wdrożenie lokalne	Wdrożenie chmurowe
▪ Lokalny serwer zarządzania ▪ Możliwość korzystania z zarówno licencji subskrypcyjnych, jak i licencji wieczystych ▪ Agent dla VMware (urządzenie wirtualne) i agent dla VMware (Windows) ▪ Optymalizacja sieci WAN pod kątem replikacji maszyn wirtualnych (seeding replik) ▪ Generator nośnika startowego ▪ Funkcje tworzenia kopii zapasowych i zarządzania dyskami na nośniku startowym ▪ Uaktualnienie ze starszych wersji programu Acronis Backup, w tym Acronis Backup for VMware ▪ Udział w programie jakości obsługi klienta firmy Acronis	▪ Zarządzanie grupami i kontami ▪ Wymóg licencji subskrypcyjnej ▪ Brak agenta dla VMware (urządzenie wirtualne) ▪ Kopie zapasowe urządzeń przenośnych w chmurze

2.2 Komponenty

Agenty

Agenty to aplikacje służące do tworzenia kopii zapasowych, odzyskiwania i wykonywania innych operacji na komputerach zarządzanych przy użyciu programu Acronis Backup.

Wybierz agenta w zależności od elementów, których kopię zapasową zamierzasz utworzyć. Poniższa tabela zawiera zestawienie informacji ułatwiających decyzję.

Uwaga: agent dla systemu Windows jest instalowany razem z agentem dla programu Exchange, agentem dla SQL oraz agentem dla usługi Active Directory. Na przykład po zainstalowaniu agenta dla SQL można utworzyć kopię zapasową całego komputera, na którym został zainstalowany ten agent.

Co chcesz uwzględnić w kopii zapasowej?	Którego agenta należy zainstalować?	Gdzie trzeba go zainstalować?	Dostępność agenta	
			Lokalnie	Chmura
Komputery fizyczne				
Dyski, woluminy i pliki na komputerach fizycznych z systemem Windows	Agent dla systemu Windows	Na komputerze, którego kopia zapasowa zostanie utworzona.	+	+
Dyski, woluminy i pliki na komputerach fizycznych z systemem Linux	Agent dla systemu Linux		+	+
Dyski, woluminy i pliki na komputerach fizycznych z systemem OS X	Agent dla systemu Mac		+	+
Aplikacje				
Bazy danych SQL	Agent dla SQL	Na komputerze z programem Microsoft SQL Server.	+	+

Copyright © Acronis International GmbH, 2002-2017

Co chcesz uwzględnić w kopii zapasowej?	Którego agenta należy zainstalować?	Gdzie trzeba go zainstalować?	Dostępność agenta	
			Lokalnie	Chmura
Bazy danych programu Exchange	Agent dla programu Exchange	Na komputerze z rolą Skrzynka pocztowa programu Microsoft Exchange Server.	+	+
Skrzynki pocztowe w usłudze Microsoft Office 365	Agent dla usługi Office 365	Na podłączonym do Internetu komputerze z systemem Windows.	+	+
Komputery z usługami domenowymi Active Directory	Agent dla usługi Active Directory	Na kontrolerze domeny.	+	+
Maszyny wirtualne				
Maszyny wirtualne VMware ESXi	Agent dla VMware (Windows)	Na komputerze z systemem Windows, który ma dostęp przez sieć do serwera vCenter oraz magazynu maszyn wirtualnych*.	+	+
	Agent dla VMware (urządzenie wirtualne)	Na hoście ESXi.	+	–
Maszyny wirtualne Hyper-V	Agent dla Hyper-V	Na hoście Hyper-V.	+	+
Maszyny wirtualne znajdujące się w środowisku Windows Azure	Tak samo jak w przypadku komputerów fizycznych**	Na komputerze, którego kopia zapasowa zostanie utworzona.	+	+
Maszyny wirtualne znajdujące się w środowisku Amazon EC2			+	+
Urządzenia mobilne				
Urządzenia mobilne z systemem Android	Aplikacja mobilna dla systemu Android	Na urządzeniu mobilnym, którego kopia zapasowa zostanie utworzona.	–	+
Urządzenia mobilne z systemem iOS	Aplikacja mobilna dla systemu iOS		–	+

* Jeśli system ESXi korzysta z pamięci masowej dołączonej do sieci SAN, zainstaluj agenta na komputerze podłączonym do tej samej sieci SAN. Agent będzie tworzył kopie zapasowe maszyn wirtualnych bezpośrednio z magazynu, a nie z hosta ESXi czy z sieci lokalnej. Aby uzyskać szczegółowe instrukcje, zobacz „Agent dla VMware — tworzenie kopii zapasowych bez obciążania sieci lokalnej” (s. 132).

** W przypadku tworzenia kopii zapasowej przez agenta zewnętrznego maszyna wirtualna jest traktowana jako maszyna wirtualna. Jeśli agent jest zainstalowany w systemie-gościu, operacje tworzenia kopii zapasowych i odzyskiwania są takie same jak w przypadku komputera fizycznego. Niemniej jednak w przypadku ustawienia limitów liczby komputerów we wdrożeniu chmurowym komputer jest traktowany jako maszyna wirtualna.

Inne komponenty

Komponent	Funkcja	Gdzie trzeba go zainstalować?	Dostępność	
			Lokalnie	Chmura

Copyright © Acronis International GmbH, 2002-2017

Komponent	Funkcja	Gdzie trzeba go zainstalować?	Dostępność	
			Lokalnie	Chmura
Serwer zarządzania	Zarządza agentami. Udostępnia użytkownikom interfejs internetowy.	Na komputerze z systemem Windows lub Linux.	+	–
Generator nośnika startowego	Tworzy nośnik startowy.	Na komputerze z systemem Windows lub Linux.	+	–
Monitor kopii zapasowych	Umożliwia użytkownikom monitorowanie kopii zapasowych poza interfejsem internetowym.	Na komputerze z systemem Windows lub OS X.	+	+
Narzędzie wiersza polecenia	Udostępnia interfejs wiersza polecenia.	Na komputerze z systemem Windows lub Linux.	+	+

2.3 Wymagania dotyczące oprogramowania

2.3.1 Obsługiwane przeglądarki internetowe

Interfejs internetowy obsługuje następujące przeglądarki internetowe:

- Google Chrome 29 lub nowsza
- Mozilla Firefox 23 lub nowsza
- Opera 16 lub nowsza
- Internet Explorer 10 lub nowsza
- Safari 5.1.7 lub nowsza w systemach operacyjnych OS X oraz iOS

W innych przeglądarkach internetowych (oraz w programie Safari działającym w innych systemach operacyjnych) interfejs użytkownika może być wyświetlany niepoprawnie lub niektóre funkcje mogą być niedostępne.

2.3.2 Obsługiwane systemy operacyjne i środowiska

2.3.2.1 Agenty

Agent dla systemu Windows

Windows XP Professional SP3 (x86, x64)

Windows Server 2003/2003 R2 — wersje Standard i Enterprise (x86, x64)

Windows Small Business Server 2003/2003 R2

Windows Vista — wszystkie wersje

Windows Server 2008 — wersje Standard, Enterprise, Datacenter i Web (x86, x64)

Windows Small Business Server 2008

Windows 7 — wszystkie wersje

Windows Server 2008 R2 — wersje Standard, Enterprise, Datacenter, Foundation i Web

Windows MultiPoint Server 2010/2011/2012

Copyright © Acronis International GmbH, 2002-2017

Windows Small Business Server 2011 — wszystkie wersje

Windows 8/8.1 — wszystkie wersje z wyjątkiem Windows RT (x86, x64)

Windows Server 2012/2012 R2 — wszystkie wersje

Windows Storage Server 2003/2008/2008 R2/2012/2012 R2

Windows 10 — wersje Home, Pro, Education i Enterprise

Windows Server 2016 — wszystkie opcje instalacji z wyjątkiem systemu Nano Server

Agent dla SQL, agent dla programu Exchange oraz agent dla usługi Active Directory

Każdy z tych agentów można zainstalować na komputerze z dowolnym wymienionym wyżej systemem operacyjnym i obsługiwaną wersją odpowiedniej aplikacji.

Agent dla usługi Office 365

Windows Server 2008 — wersje Standard, Enterprise, Datacenter i Web (tylko x64)

Windows Small Business Server 2008

Windows Server 2008 R2 — wersje Standard, Enterprise, Datacenter, Foundation i Web

Windows Small Business Server 2011 — wszystkie wersje

Windows 8/8.1 — wszystkie wersje z wyjątkiem Windows RT (tylko x64)

Windows Server 2012/2012 R2 — wszystkie wersje

Windows Storage Server 2008/2008 R2/2012/2012 R2 (tylko x64)

Windows 10 — wersje Home, Pro, Education i Enterprise (tylko x64)

Windows Server 2016 — wszystkie opcje instalacji z wyjątkiem systemu Nano Server (tylko x64)

Agent dla systemu Linux

System Linux z jądrem w wersji od 2.6.9 do 4.9 i biblioteką glibc w wersji 2.3.4 lub nowszej

Różne dystrybucje x86 i x86_64 systemu Linux, w tym:

- Red Hat Enterprise Linux 4.x, 5.x, 6.x, 7.0, 7.1, 7.2, 7.3
- Ubuntu 9.10, 10.04, 10.10, 11.04, 11.10, 12.04, 12.10, 13.04, 13.10, 14.04, 14.10, 15.04, 15.10, 16.04
- Fedora 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23
- SUSE Linux Enterprise Server 10 i 11
- SUSE Linux Enterprise Server 12 — obsługa w systemach plików, z wyjątkiem Btrfs
- Debian 4, 5, 6, 7.0, 7.2, 7.4, 7.5, 7.6, 7.7, 8.0, 8.1, 8.2, 8.3, 8.4, 8.5
- CentOS 5.x, 6.x, 7, 7.1, 7.2, 7.3
- Oracle Linux 5.x, 6.x, 7.0, 7.1, 7.2, 7.3 — wersje Unbreakable Enterprise Kernel i Red Hat Compatible Kernel
- CloudLinux 5.x, 6.x, 7, 7.1
- ClearOS 5.x, 6.x, 7, 7.1

Przed zainstalowaniem programu w systemie, który nie używa menedżera RPM Package Manager, np. Ubuntu, należy ręcznie zainstalować ten menedżer (jako użytkownik root), na przykład przy użyciu następującego polecenia: **`apt-get install rpm`**

Agent dla systemu Mac

OS X Mountain Lion 10.8

OS X Mavericks 10.9

OS X Yosemite 10.10

Copyright © Acronis International GmbH, 2002-2017

OS X El Capitan 10.11

macOS Sierra 10.12 — Apple File System (APFS) nie jest obsługiwany

Agent dla VMware (urządzenie wirtualne)

Ten agent jest udostępniany jako urządzenie wirtualne do uruchomienia na hoście ESXi.

VMware ESXi 4.1, 5.0, 5.1, 5.5, 6.0 i 6.5

Agent dla VMware (Windows)

Ten agent jest udostępniany jako aplikacja systemu Windows do uruchomienia w dowolnym z systemów operacyjnych wymienionych powyżej w obszarze Agent dla systemu Windows z następującymi wyjątkami:

- 32-bitowe systemy operacyjne nie są obsługiwane.
- Systemy Windows XP, Windows Server 2003/2003 R2 i Windows Small Business Server 2003/2003 R2 nie są obsługiwane.

Agent dla Hyper-V

Windows Server 2008 (x64) z rolą Hyper-V

Windows Server 2008 R2 z rolą Hyper-V

Microsoft Hyper-V Server 2008/2008 R2

Windows Server 2012/2012 R2 z rolą Hyper-V

Microsoft Hyper-V Server 2012/2012 R2

Windows 8, 8.1 (x64) z rolą Hyper-V

Windows 10 — wersje Pro, Education i Enterprise z rolą Hyper-V

Windows Server 2016 z rolą Hyper-V — wszystkie opcje instalacji z wyjątkiem systemu Nano Server

Microsoft Hyper-V Server 2016

2.3.2.2 Serwer zarządzania (tylko w ramach wdrożenia lokalnego)

W systemie Windows

Windows Server 2008 — wersje Standard, Enterprise i Datacenter (x86, x64)

Windows Small Business Server 2008

Windows 7 — wszystkie wersje (x86, x64)

Windows Server 2008 R2 — wersje Standard, Enterprise, Datacenter i Foundation

Windows MultiPoint Server 2010/2011/2012

Windows Small Business Server 2011 — wszystkie wersje

Windows 8/8.1 — wszystkie wersje z wyjątkiem Windows RT (x86, x64)

Windows Server 2012/2012 R2 — wszystkie wersje

Windows Storage Server 2008/2008 R2/2012/2012 R2

Windows 10 — wersje Home, Pro, Education i Enterprise

Windows Server 2016 — wszystkie opcje instalacji z wyjątkiem systemu Nano Server

W systemie Linux

System Linux z jądrem w wersjach od 2.6.18 do 4.9 i biblioteką glibc w wersji 2.3.4 lub nowszej

Różne dystrybucje systemu Linux x86_64, w tym:

Red Hat Enterprise Linux 4.x, 5.x, 6.x, 7.0, 7.1, 7.2, 7.3

Copyright © Acronis International GmbH, 2002-2017

Ubuntu 9.10, 10.04, 10.10, 11.04, 11.10, 12.04, 12.10, 13.04, 13.10, 14.04, 14.10, 15.04, 15.10, 16.04

Fedora 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23

SUSE Linux Enterprise Server 10, 11, 12

Debian 4, 5, 6, 7.0, 7.2, 7.4, 7.5, 7.6, 7.7, 8.0, 8.1, 8.2, 8.3, 8.4, 8.5

CentOS 5.x, 6.x, 7, 7.1, 7.2, 7.3

Oracle Linux 5.x, 6.x, 7.0, 7.1, 7.2, 7.3 — wersje Unbreakable Enterprise Kernel i Red Hat Compatible Kernel

CloudLinux 5.x, 6.x, 7, 7.1

2.3.3 Obsługiwane wersje programu Microsoft SQL Server

- Microsoft SQL Server 2016
- Microsoft SQL Server 2014
- Microsoft SQL Server 2012
- Microsoft SQL Server 2008 R2
- Microsoft SQL Server 2008
- Microsoft SQL Server 2005

2.3.4 Obsługiwane wersje programu Microsoft Exchange Server

- **Microsoft Exchange Server 2016** — wszystkie wersje.
- **Microsoft Exchange Server 2013** — wszystkie wersje, aktualizacja Cumulative Update 1 (CU1) i nowsze.
- **Microsoft Exchange Server 2010** — wszystkie wersje, wszystkie dodatki Service Pack. Odzyskiwanie skrzynek pocztowych i ich elementów jest obsługiwane od czasu wprowadzenia dodatku Service Pack 1 (SP1).
- **Microsoft Exchange Server 2007** — wszystkie wersje, wszystkie dodatki Service Pack. Odzyskiwanie skrzynek pocztowych i ich elementów nie jest obsługiwane.

2.3.5 Obsługiwane wersje programu Microsoft SharePoint

Program Acronis Backup 12 obsługuje następujące wersje programu Microsoft SharePoint:

- Microsoft SharePoint 2013
- Microsoft SharePoint Server 2010 SP1
- Microsoft SharePoint Foundation 2010 SP1
- Microsoft Office SharePoint Server 2007 SP2*
- Microsoft Windows SharePoint Services 3.0 SP2*

*Aby można było używać narzędzia SharePoint Explorer z tymi wersjami, musi być dostępna farma odzyskiwania programu SharePoint, do której będzie można dołączyć bazy danych.

Kopie zapasowe lub bazy danych, z których są wyodrębniane dane, muszą pochodzić z tej samej wersji programu SharePoint co wersja, w której jest zainstalowane narzędzie SharePoint Explorer.

2.3.6 Obsługiwane platformy wirtualizacji

W poniższej tabeli zestawiono możliwości obsługi poszczególnych platform wirtualizacji.

Copyright © Acronis International GmbH, 2002-2017

Platforma	Tworzenie kopii zapasowych na poziomie hiperwizora	Tworzenie kopii zapasowych w ramach systemu operacyjnego-gościa
VMware		
Wersje środowiska VMware vSphere: 4.1, 5.0, 5.1, 5.5, 6.0, 6.5 **Wersje środowiska VMware vSphere:** VMware vSphere Essentials* VMware vSphere Essentials Plus* VMware vSphere Standard* VMware vSphere Advanced VMware vSphere Enterprise VMware vSphere Enterprise Plus	+	+
VMware vSphere Hypervisor (Free ESXi)**		+
VMware Server (serwer VMware Virtual) VMware Workstation VMware ACE VMware Player		+
Microsoft		
Windows Server 2008 (x64) z rolą Hyper-V Windows Server 2008 R2 z rolą Hyper-V Microsoft Hyper-V Server 2008/2008 R2 Windows Server 2012/2012 R2 z rolą Hyper-V Microsoft Hyper-V Server 2012/2012 R2 Windows 8, 8.1 (x64) z rolą Hyper-V Windows 10 z technologią Hyper-V Windows Server 2016 z rolą Hyper-V — wszystkie opcje instalacji z wyjątkiem systemu Nano Server Microsoft Hyper-V Server 2016	+	+
Microsoft Virtual PC 2004 i 2007 Windows Virtual PC		+
Microsoft Virtual Server 2005		+
Parallels		
Parallels Workstation		+
Parallels Server 4 Bare Metal		+
Amazon		
Instancje środowiska Amazon EC2		+

Copyright © Acronis International GmbH, 2002-2017

Platforma	Tworzenie kopii zapasowych na poziomie hiperwizora	Tworzenie kopii zapasowych w ramach systemu operacyjnego-gościa
Microsoft Azure		
Maszyny wirtualne Azure		+

* W tych edycjach transport HotAdd w przypadku dysków wirtualnych jest obsługiwany przez środowisko vSphere w wersji 5.0 lub nowszej. W wersji 4.1 operacje tworzenia kopii zapasowych mogą być wolniej realizowane.

** Tworzenie kopii zapasowych na poziomie hiperwizora nie jest obsługiwane w przypadku programu vSphere Hypervisor, ponieważ ogranicza on dostęp do interfejsu Remote Command Line Interface (RCLI) do trybu tylko do odczytu. Agent działa w trakcie okresu próbnego programu vSphere Hypervisor przed wprowadzeniem klucza seryjnego. Po wprowadzeniu klucza seryjnego agent przestaje działać.

Ograniczenia

- **Komputery odporne na awarie**

  Agent dla VMware tworzy kopię zapasową komputera odpornego na awarie tylko wtedy, gdy w środowisku VMware vSphere w wersji 6.0 lub nowszej została włączona odporność na awarie. Jeśli środowisko vSphere zostało uaktualnione ze starszej wersji, wystarczy na każdym komputerze wyłączyć i włączyć odporność na awarie. Jeśli korzystasz ze starszej wersji środowiska vSphere, zainstaluj agenta systemie operacyjnym-gościu.

- **Dyski niezależne i RDM**

  Agent dla VMware nie tworzy kopii zapasowych dysków Raw Device Mapping (RDM) w trybie kompatybilności fizycznej ani dysków niezależnych. Agent pomija te dyski i dodaje ostrzeżenia do dziennika. Ostrzeżeń tych można uniknąć, wykluczając dyski niezależne i RDM w trybie kompatybilności fizycznej z planu tworzenia kopii zapasowych. Aby utworzyć kopię zapasową tych dysków lub znajdujących się na nich danych, zainstaluj agenta w systemie operacyjnym-gościu.

- **Dyski pass-through**

  Agent dla Hyper-V nie tworzy kopii zapasowych dysków pass-through. Podczas tworzenia kopii zapasowej agent pomija te dyski i dodaje ostrzeżenia do dziennika. Ostrzeżeń tych można uniknąć, wykluczając dyski pass-through z planu tworzenia kopii zapasowych. Aby utworzyć kopię zapasową tych dysków lub znajdujących się na nich danych, zainstaluj agenta w systemie operacyjnym-gościu.

- **Szyfrowane maszyny wirtualne** (wprowadzone w środowisku VMware vSphere 6.5)
  - Szyfrowane maszyny wirtualne są zapisywane w kopii zapasowej w stanie niezaszyfrowanym. Jeśli szyfrowanie jest niezbędne, włącz szyfrowanie kopii zapasowych podczas tworzenia planu tworzenia kopii zapasowych (s. 53).
  - Odzyskane maszyny wirtualne nigdy nie są zaszyfrowane. Po zakończeniu odzyskiwania można szyfrowanie włączyć ręcznie.
  - Jeśli tworzysz kopie zapasowe szyfrowanych maszyn wirtualnych, zalecamy zaszyfrowanie również maszyny, na której działa agent dla VMware. W przeciwnym razie tempo operacji dotyczących szyfrowanych maszyn może być poniżej oczekiwań. Zastosuj **Zasady szyfrowania maszyn wirtualnych** do maszyny agenta przy użyciu klienta internetowego vSphere.
  - Kopie zapasowe szyfrowanych maszyn wirtualnych zostaną utworzone przy użyciu sieci lokalnej nawet w przypadku skonfigurowania dla agenta trybu transportu SAN. Ponieważ środowisko VMware nie obsługuje tworzenia kopii zapasowych zaszyfrowanych dysków

 Copyright © Acronis International GmbH, 2002-2017

wirtualnych w trybie transportu SAN, agent wykona przełączenie awaryjne na tryb transportu NBD.

- **Funkcja Secure Boot** (wprowadzona w środowisku VMware vSphere 6.5)

  Po odzyskaniu maszyny wirtualnej jako nowej maszyny funkcja **Secure Boot** jest wyłączona. Po zakończeniu odzyskiwania można tę opcję włączyć ręcznie.

2.3.7 Pakiety systemu Linux

Aby dodać potrzebne moduły do jądra systemu Linux, program instalacyjny wymaga następujących pakietów systemu Linux:

- Pakiet z nagłówkami lub źródłami jądra. Wersja pakietu musi odpowiadać wersji jądra.
- System kompilatora GNU Compiler Collection (GCC). Wersja kompilatora GCC musi być taka sama jak ta, przy użyciu której skompilowano jądro.
- Narzędzie Make.
- Interpreter języka Perl.

Nazwy tych pakietów mogą się różnić w zależności od dystrybucji systemu Linux.

W systemach Red Hat Enterprise Linux, CentOS i Fedora pakiety te są normalnie instalowane przez program instalacyjny. W pozostałych dystrybucjach pakiety te należy zainstalować, jeśli nie są jeszcze zainstalowane lub nie występują w wymaganych wersjach.

Czy wymagane pakiety są już zainstalowane?

Aby sprawdzić, czy pakiety są już zainstalowane, wykonaj następujące czynności:

1. Uruchom następujące polecenie, aby poznać wersję jądra i wymaganą wersję kompilatora GCC:

   ```
   cat /proc/version
   ```

   Wynikiem działania tego polecenia są wiersze podobne do następujących: **`Linux version 2.6.35.6`** i **`gcc version 4.5.1`**
2. Uruchom następujące polecenie, aby sprawdzić, czy jest zainstalowane narzędzie Make i kompilator GCC:

   ```
   make -v
   gcc -v
   ```

   W przypadku kompilatora **gcc** sprawdź, czy wersja zwrócona przez polecenie jest taka sama jak wersja **`gcc version`** w kroku 1. W przypadku narzędzia **make** wystarczy sprawdzić, czy polecenie uruchamia się.
3. Sprawdź, czy jest zainstalowana odpowiednia wersja pakietów do kompilowania modułów jądra:
   - W systemach Red Hat Enterprise Linux, CentOS i Fedora uruchom następujące polecenie:

     ```
     yum list installed | grep kernel-devel
     ```
   - W systemie Ubuntu uruchom następujące polecenia:

     ```
     dpkg --get-selections | grep linux-headers
     dpkg --get-selections | grep linux-image
     ```

   W obu przypadkach sprawdź, czy wersje pakietów są takie same jak wersja **`Linux version`** w kroku 1.
4. Uruchom następujące polecenie, aby sprawdzić, czy jest zainstalowany interpreter języka Perl:

   ```
   perl --version
   ```

   Jeśli zostanie wyświetlona informacja o wersji języka Perl, interpreter jest zainstalowany.

Copyright © Acronis International GmbH, 2002-2017

Instalowanie pakietów z repozytorium

Poniższa tabela przedstawia sposoby instalacji wymaganych pakietów w różnych dystrybucjach systemu Linux.

Dystrybucja systemu Linux	Nazwy pakietów	Sposób instalacji
Red Hat Enterprise Linux	**kernel-devel** **gcc** **make**	Program instalacyjny automatycznie pobierze i zainstaluje pakiety z użyciem subskrypcji Red Hat.
	perl	Uruchom następujące polecenie: `yum install perl`
CentOS Fedora	**kernel-devel** **gcc** **make**	Program instalacyjny automatycznie pobierze i zainstaluje pakiety.
	perl	Uruchom następujące polecenie: `yum install perl`
Ubuntu	**linux-headers** **linux-image** **gcc** **make** **perl**	Uruchom następujące polecenia: `sudo apt-get update` `sudo apt-get install linux-headers-`uname -r`` `sudo apt-get install linux-image-`uname -r`` `sudo apt-get install gcc-<package version>` `sudo apt-get install make` `sudo apt-get install perl`

Pakiety zostaną pobrane z repozytorium dystrybucji i zainstalowane.

W przypadku innych dystrybucji systemu Linux dokładne nazwy wymaganych pakietów i metody ich instalacji można znaleźć w dokumentacji dystrybucji.

Ręczne instalowanie pakietów

Ręczna instalacja pakietów może być konieczna w następujących przypadkach:

- Komputer nie ma aktywnej subskrypcji Red Hat lub połączenia z Internetem.
- Program instalacyjny nie może znaleźć wersji pakietów **kernel-devel** lub **gcc** odpowiadających wersji jądra. Jeśli dostępny pakiet **kernel-devel** jest nowszy niż jądro, należy ręcznie zaktualizować jądro lub zainstalować odpowiednią wersję pakietu **kernel-devel**.
- Użytkownik ma wymagane pakiety w sieci lokalnej i nie chce tracić czasu na ich automatyczne wyszukiwanie i pobieranie.

Uzyskaj pakiety z sieci lokalnej lub z witryny internetowej zaufanej innej firmy i zainstaluj je zgodnie z poniższymi wskazówkami:

- W systemie Red Hat Enterprise Linux, CentOS lub Fedora uruchom jako użytkownik root następujące polecenie:
  ```
  rpm -ivh PACKAGE_FILE1 PACKAGE_FILE2 PACKAGE_FILE3
  ```
- W systemie Ubuntu uruchom następujące polecenie:
  ```
  sudo dpkg -i PACKAGE_FILE1 PACKAGE_FILE2 PACKAGE_FILE3
  ```


Copyright © Acronis International GmbH, 2002-2017

Przykład: ręczne instalowanie pakietów w systemie Fedora 14

Wykonaj następujące czynności, aby zainstalować wymagane pakiety w systemie Fedora 14 na komputerze 32-bitowym:

1. Uruchom następujące polecenie, aby określić wersję jądra i wymaganą wersję kompilatora GCC:

   ```
   cat /proc/version
   ```

   W wyniku jego uruchomienia zostają zwrócone następujące informacje:

   ```
   Linux version 2.6.35.6-45.fc14.i686
   gcc version 4.5.1
   ```

2. Uzyskaj pakiety **kernel-devel** i **gcc** odpowiadające tej wersji jądra:

   ```
   kernel-devel-2.6.35.6-45.fc14.i686.rpm
   gcc-4.5.1-4.fc14.i686.rpm
   ```

3. Uzyskaj pakiet **make** dla systemu Fedora 14:

   ```
   make-3.82-3.fc14.i686
   ```

4. Zainstaluj pakiety, uruchamiając jako użytkownik root następujące polecenie:

   ```
   rpm -ivh kernel-devel-2.6.35.6-45.fc14.i686.rpm
   rpm -ivh gcc-4.5.1.fc14.i686.rpm
   rpm -ivh make-3.82-3.fc14.i686
   ```

   Wszystkie wspomniane pakiety można określić w pojedynczym poleceniu **`rpm`**. Zainstalowanie każdego z pakietów może wymagać instalacji dodatkowych pakietów wynikających z określonych zależności.

2.3.8 Kompatybilność z programami szyfrującymi

W przypadku tworzenia kopii zapasowych i odzyskiwania danych szyfrowanych za pomocą oprogramowania szyfrującego *na poziomie plików* nie występują żadne ograniczenia.

Oprogramowanie szyfrujące *na poziomie dysku* szyfruje dane w locie. Dlatego dane w kopii zapasowej są w postaci niezaszyfrowanej. Programy szyfrujące na poziomie dysku często modyfikują obszary systemowe: rekordy rozruchowe, tabele partycji lub tabele systemów plików. Te czynniki wpływają na tworzenie kopii zapasowych na poziomie dysku i odzyskiwanie z nich danych, a także możliwości uruchamiania odzyskanego systemu i dostępu do strefy Secure Zone.

Można tworzyć kopie zapasowe danych zaszyfrowanych przy użyciu następujących programów szyfrujących na poziomie dysku:

- Microsoft BitLocker Drive Encryption
- McAfee Endpoint Encryption
- PGP Whole Disk Encryption.

Aby zapewnić niezawodne odzyskiwanie na poziomie dysku, postępuj zgodnie z powszechnymi regułami oraz zaleceniami dotyczącymi konkretnych programów.

Powszechna reguła dotycząca instalacji

Stanowczo zaleca się zainstalowanie oprogramowania szyfrującego przed instalacją agentów kopii zapasowych.

Sposób korzystania ze strefy Secure Zone

Strefy Secure Zone nie można zaszyfrować na poziomie dysku. Ze strefy Secure Zone można korzystać tylko w następujący sposób:

Copyright © Acronis International GmbH, 2002-2017

1. Zainstaluj oprogramowanie szyfrujące, a następnie zainstaluj agenta.
2. Utwórz strefę Secure Zone.
3. Wyklucz strefę Secure Zone w przypadku szyfrowania dysku lub jego woluminów.

Powszechna reguła dotycząca tworzenia kopii zapasowych

Kopię zapasową na poziomie dysku można utworzyć pod kontrolą systemu operacyjnego. Nie próbuj utworzyć kopii zapasowej przy użyciu nośnika startowego.

Procedury odzyskiwania dotyczące konkretnych programów

Microsoft BitLocker Drive Encryption

Aby odzyskać system zaszyfrowany przez program BitLocker:

1. Uruchom komputer za pomocą nośnika startowego.
2. Odzyskaj system. Odzyskane dane będą w postaci niezaszyfrowanej.
3. Ponownie uruchom odzyskany system.
4. Włącz program BitLocker.

Jeśli musisz odzyskać tylko jedną z wielu partycji dysku, wykonaj tę operację pod kontrolą systemu operacyjnego. Odzyskiwanie za pomocą nośnika startowego może spowodować, że odzyskana partycja nie będzie wykrywana w systemie Windows.

McAfee Endpoint Encryption i PGP Whole Disk Encryption

Zaszyfrowaną partycję systemową można odzyskać tylko przy użyciu nośnika startowego.

Jeśli odzyskany system się nie uruchomi, odbuduj główny rekord startowy zgodnie z opisem podanym w artykule bazy wiedzy Microsoft Knowledge Base: https://support.microsoft.com/kb/2622803.

2.4 Wymagania systemowe

W poniższej tabeli zestawiono wymagania dotyczące miejsca na dysku oraz pamięci w typowych instalacjach. Instalacja jest wykonywana przy użyciu ustawień domyślnych.

Komponenty do zainstalowania	Zajmowane miejsce na dysku	Minimalne zużycie pamięci
Agent dla systemu Windows	850 MB	150 MB
Agent dla systemu Windows i jeden z następujących agentów: ▪ Agent dla SQL ▪ Agent dla programu Exchange	950 MB	170 MB
Agent dla systemu Windows i jeden z następujących agentów: ▪ Agent dla VMware (Windows) ▪ Agent dla Hyper-V	1170 MB	180 MB
Agent dla usługi Office 365	500 MB	170 MB
Agent dla systemu Linux	720 MB	130 MB
Agent dla systemu Mac	500 MB	150 MB
Tylko w przypadku wdrożeń lokalnych		
Serwer zarządzania w systemie Windows	1,7 GB	200 MB

Copyright © Acronis International GmbH, 2002-2017

Serwer zarządzania w systemie Linux	0,6 GB	200 MB
Serwer zarządzania i agent dla systemu Windows	2,4 GB	360 MB
Serwer zarządzania i agenty na komputerze z systemem Windows oraz oprogramowaniem Microsoft SQL Server i Microsoft Exchange Server oraz Usługami domenowymi Active Directory	3,35 GB	400 MB
Serwer zarządzania i agent dla systemu Linux	1,2 GB	340 MB

Podczas tworzenia kopii zapasowej agent zwykle używa około 350 MB pamięci (pomiaru dokonano podczas tworzenia kopii zapasowej danych o objętości 500 GB). Szczytowe zużycie może sięgnąć 2 GB, zależnie od ilości i typu przetwarzanych danych.

Nośnik startowy lub odzyskiwanie z dysku z ponownym uruchomieniem wymaga co najmniej 1 GB pamięci.

Serwer zarządzania z jednym zarejestrowanym komputerem używa 200 MB pamięci. Każdy nowo zarejestrowany komputer używa dodatkowo około 4 MB. W związku z tym serwer ze 100 zarejestrowanymi komputerami używa około 600 MB ponad to, czego używa system operacyjny i uruchomione aplikacje. Maksymalna liczba zarejestrowanych komputerów wynosi 900–1000. Ograniczenie to wynika z wbudowanej w serwer zarządzania bazy SQLite.

2.5 Obsługiwane systemy plików

Agent kopii zapasowych może tworzyć kopie zapasowe każdego systemu plików dostępne z systemu operacyjnego, w którym ten agent jest zainstalowany. Na przykład agent dla systemu Windows może tworzyć kopie zapasowe systemu plików ext4 i go odzyskiwać, jeśli w systemie Windows jest zainstalowany odpowiedni sterownik.

W poniższej tabeli zestawiono systemy plików, które można uwzględniać w kopiach zapasowych i odzyskiwać. Ograniczenia dotyczą zarówno agentów, jak i nośnika startowego.

<table>
<tr><th rowspan="2">System plików</th><th colspan="4">Obsługujące agenty i nośniki</th><th rowspan="2">Ograniczenia</th></tr>
<tr><th>Agenty</th><th>Nośnik startowy środowiska Win-PE</th><th>Nośnik startowy oparty na systemie Linux</th><th>Nośnik startowy systemu Mac</th></tr>
<tr><td>FAT16/32</td><td rowspan="3">Wszystkie agenty</td><td>+</td><td>+</td><td>+</td><td rowspan="4">Brak ograniczeń</td></tr>
<tr><td>NTFS</td><td>+</td><td>+</td><td>+</td></tr>
<tr><td>ext2/ext3/ext4</td><td>+</td><td>+</td><td>-</td></tr>
<tr><td>HFS+</td><td>Agent dla systemu Mac</td><td>-</td><td>-</td><td>+</td></tr>
<tr><td>JFS</td><td rowspan="2">Agent dla systemu Linux</td><td>-</td><td>+</td><td>-</td><td rowspan="2">Z kopii zapasowej dysku nie można wykluczać plików</td></tr>
<tr><td>ReiserFS3</td><td>-</td><td>+</td><td>-</td></tr>
</table>

Copyright © Acronis International GmbH, 2002-2017

System plików	Obsługujące agenty i nośniki				Ograniczenia
	Agenty	Nośnik startowy środowiska Win-PE	Nośnik startowy oparty na systemie Linux	Nośnik startowy systemu Mac	
ReiserFS4	Wszystkie agenty	-	+	-	▪ Z kopii zapasowej dysku nie można wykluczać plików ▪ Podczas odzyskiwania nie można zmieniać rozmiarów woluminów
ReFS		+	+	+	
XFS		+	+	+	
Linux Swap	Agent dla systemu Linux	-	+	-	Brak ograniczeń

W przypadku tworzenia kopii zapasowej dysków z nierozpoznanym lub nieobsługiwanym systemem plików oprogramowanie automatycznie przełącza się na tryb „sektor po sektorze”. Kopię zapasową sektor po sektorze można utworzyć w przypadku każdego systemu plików, który spełnia następujące warunki:

- jest oparty na blokach
- obejmuje jeden dysk
- ma standardowy schemat partycjonowania MBR/GPT

Jeśli system plików nie spełnia tych wymagań, operacja tworzenia kopii zapasowej się nie powiedzie.

2.6 Wdrożenie lokalne

2.6.1 Instalowanie serwera zarządzania

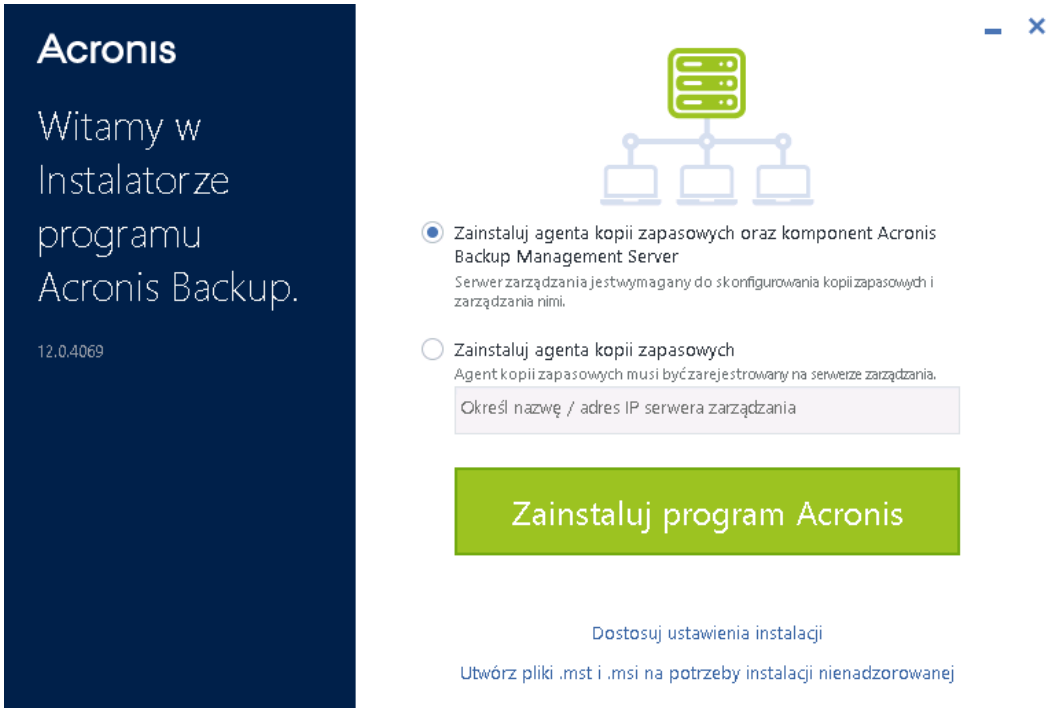
2.6.1.1 Instalacja w systemie Windows

Aby zainstalować serwer zarządzania

1. Zaloguj się jako administrator i uruchom program instalacyjny produktu Acronis Backup.
2. [Opcjonalnie] Aby zmienić język, w którym jest wyświetlany program instalacyjny, kliknij **Skonfiguruj język**.
3. Zaakceptuj warunki umowy licencyjnej i określ, czy komputer ma zostać objęty programem jakości obsługi klienta firmy Acronis.

Copyright © Acronis International GmbH, 2002-2017

4. Zostaw domyślne ustawienie **Zainstaluj agenta kopii zapasowych oraz komponent Acronis Backup Management Server**.



   Domyślnie zostaną zainstalowane następujące komponenty:

   - Serwer zarządzania
   - Agent dla systemu Windows
   - Inne agenty (agent dla Hyper-V, agent dla programu Exchange, agent dla SQL oraz agent dla usługi Active Directory), jeśli na komputerze zostaną wykryte odpowiedni hiperwizor lub odpowiednia aplikacja
   - Generator nośnika startowego
   - Narzędzie wiersza polecenia
   - Monitor kopii zapasowych

   Możesz skonfigurować instalację, klikając **Dostosuj ustawienia instalacji**.
5. Kontynuuj instalację.
6. Po zakończeniu instalacji kliknij **Zamknij**. W domyślnej przeglądarce internetowej zostanie otwarta konsola kopii zapasowych.

2.6.1.2 Instalacja w systemie Linux

Przygotowanie

1. Przed zainstalowaniem programu w systemie, który nie używa menedżera RPM Package Manager, np. Ubuntu, należy ręcznie zainstalować ten menedżer (jako użytkownik root), na przykład przy użyciu następującego polecenia: **`apt-get install rpm`**.
2. Aby razem z serwerem zarządzania zainstalować agenta dla systemu Linux, upewnij się, że na komputerze są zainstalowane niezbędne pakiety systemu Linux (s. 17).

Instalacja

Aby zainstalować serwer zarządzania

1. Uruchom plik instalacyjny jako użytkownik root.
2. Zaakceptuj warunki umowy licencyjnej.

Copyright © Acronis International GmbH, 2002-2017

3. [Opcjonalnie] Wybierz komponenty, które chcesz zainstalować.

   Domyślnie zostaną zainstalowane następujące komponenty:

   - Serwer zarządzania
   - Agent dla systemu Linux
   - Generator nośnika startowego
4. Określ port, którego przeglądarka internetowa będzie używać w celu uzyskania dostępu do serwera zarządzania. Wartość domyślna to 9877.
5. Określa port, który będzie używany do komunikacji między komponentami produktu. Wartość domyślna to 7780.
6. Kliknij **Dalej**, aby kontynuować instalację.
7. Po zakończeniu instalacji wybierz **Otwórz konsolę internetową**, a następnie kliknij **Wyjście**. W domyślnej przeglądarce internetowej zostanie otwarta konsola kopii zapasowych.

2.6.2 Dodawanie komputerów przy użyciu interfejsu internetowego

Aby rozpocząć dodawanie komputera do serwera zarządzania, kliknij **Wszystkie urządzenia** > **Dodaj**.

Jeśli serwer zarządzania został zainstalowany w systemie Linux, pojawi się monit o wybranie programu instalacyjnego zgodnego z typem dodawanego komputera. Po pobraniu programu instalacyjnego uruchom go lokalnie na danym komputerze.

Operacje opisane w dalszej części tej sekcji można wykonać pod warunkiem zainstalowania serwera zarządzania w systemie Windows. W większości przypadków agent zostanie wdrożony w trybie dyskretnym na wybranym komputerze.

2.6.2.1 Dodawanie komputera z systemem Windows

Przygotowanie

1. Aby pomyślnie przeprowadzić instalację na komputerze zdalnym z systemem Windows XP, musi być na nim *wyłączona* opcja **Panel sterowania > Opcje folderów > Widok > Użyj prostego udostępniania plików**.

   Aby pomyślnie przeprowadzić instalację na komputerze zdalnym z systemem Windows Vista lub nowszym, musi być na nim *wyłączona* opcja **Panel sterowania > Opcje folderów > Widok > Użyj Kreatora udostępniania**.
2. Aby pomyślnie przeprowadzić instalację na komputerze zdalnym, który *nie* należy do domeny Active Directory, musi być na nim *wyłączona* funkcja Kontrola konta użytkownika (UAC) (s. 25).
3. Na komputerze zdalnym należy *włączyć* udostępnianie plików i drukarek. Aby uzyskać dostęp do tej opcji:
   - Na komputerze z systemem Windows XP z dodatkiem Service Pack 2 lub Windows 2003 Server: wybierz **Panel sterowania > Zapora systemu Windows > Wyjątki > Udostępnianie plików i drukarek**.
   - Na komputerze z systemem Windows Vista, Windows Server 2008, Windows 7 lub nowszym: wybierz **Panel sterowania > Zapora systemu Windows > Centrum sieci i udostępniania > Zmień zaawansowane ustawienia udostępniania**.
4. Na potrzeby instalacji zdalnej program Acronis Backup używa portów TCP 445 i 25001. Ponadto do instalacji zdalnej i do komunikacji między komponentami służy port TCP 9876.

Copyright © Acronis International GmbH, 2002-2017

Port 445 jest automatycznie otwierany po wybraniu opcji Udostępnianie plików i drukarek. Porty 9876 i 25001 są automatycznie otwierane przez Zaporę systemu Windows. W przypadku korzystania z innej zapory sprawdź, czy porty te są otwarte (dodane do listy wyjątków) zarówno dla żądań przychodzących, jak i wychodzących.

Po zakończeniu instalacji zdalnej możesz usunąć porty 445 i 25001 z listy wyjątków. Port 25001 jest automatycznie zamykany przez Zaporę systemu Windows. Port 9876 musi pozostać otwarty.

Dodawanie komputera

1. Kliknij **Wszystkie urządzenia** > **Dodaj**.
2. Kliknij **Windows** lub przycisk odpowiadający aplikacji, którą chcesz chronić. W zależności od kliknięty przycisku zostanie wybrana jedna z następujących opcji:
   - Agent dla systemu Windows
   - Agent dla Hyper-V
   - Agent dla SQL + agent dla systemu Windows
   - Agent dla programu Exchange + agent dla systemu Windows
   - Agent dla usługi Active Directory + agent dla systemu Windows
   - Agent dla usługi Office 365
3. Określ nazwę hosta lub adres IP komputera oraz poświadczenia znajdującego się na tym komputerze konta z uprawnieniami administracyjnymi.
4. Kliknij **Dodaj**.

Wymagania dotyczące funkcji Kontrola konta użytkownika (UAC)

Na komputerze, który działa pod kontrolą systemu operacyjnego Windows Vista lub nowszego i który nie należy do domeny Active Directory, trzeba wyłączyć funkcję UAC, aby zapewnić prawidłowy przebieg operacji zarządzania scentralizowanego (w tym instalacji zdalnej).

Aby wyłączyć funkcję UAC

Zależnie od wersji systemu operacyjnego wykonaj jedną z następujących czynności:

- **W systemie operacyjnym Windows starszym niż Windows 8:**

  Przejdź do **Panel sterowania > Widok: Małe ikony > Konta użytkowników > Zmień ustawienia funkcji Kontrola konta użytkownika**, a następnie przesuń suwak w położenie **Nie powiadamiaj nigdy**. Następnie uruchom ponownie komputer.
- **W każdym systemie operacyjnym Windows**:
  1. Uruchom Edytor rejestru.
  2. Odszukaj następujący klucz rejestru:
     HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System
  3. Zmień wartość **EnableLUA** na **0**.
  4. Uruchom ponownie komputer.

2.6.2.2 Dodawanie komputera z systemem Linux

1. Kliknij **Wszystkie urządzenia** > **Dodaj**.
2. Kliknij **Linux**. Spowoduje to pobranie pliku instalacyjnego.
3. Na komputerze, który chcesz objąć ochroną, uruchom lokalnie program instalacyjny (s. 29).

2.6.2.3 Dodawanie komputera z systemem OS X

1. Kliknij **Wszystkie urządzenia** > **Dodaj**.

Copyright © Acronis International GmbH, 2002-2017

2. Kliknij **Mac**. Spowoduje to pobranie pliku instalacyjnego.
3. Na komputerze, który chcesz objąć ochroną, uruchom lokalnie program instalacyjny (s. 29).

2.6.2.4 Dodawanie serwera vCenter lub hosta ESXi

Dostępne są trzy metody dodawania serwera vCenter lub autonomicznego hosta ESXi do serwera zarządzania:

- Wdrażanie agenta dla VMware (urządzenie wirtualne) (s. 26)

  Ta metoda jest zalecana w większości przypadków. Urządzenie wirtualne zostanie automatycznie wdrożone na każdym hoście zarządzanym przez określony serwer vCenter. Możesz wybrać hosty i dostosować ustawienia urządzenia wirtualnego.
- Instalowanie agenta dla VMware (Windows) (s. 27)

  Na potrzeby odciążonego tworzenia kopii zapasowych (tj. bez obciążania sieci lokalnej) można zainstalować agenta dla VMware na komputerze fizycznym z systemem Windows. Agent zostanie automatycznie wdrożony na określonym komputerze.
  - **Odciążone tworzenie kopii zapasowej**

    Z tej funkcji należy skorzystać, jeśli produkcyjne hosty ESXi są tak bardzo obciążone, że uruchomienie urządzeń wirtualnych jest niepożądane.
  - **Tworzenie kopii zapasowych bez obciążania sieci lokalnej**

    Jeśli system ESXi korzysta z pamięci masowej dołączonej do sieci SAN, zainstaluj agenta na komputerze podłączonym do tej samej sieci SAN. Agent będzie tworzył kopie zapasowe maszyn wirtualnych bezpośrednio z magazynu, a nie z hosta ESXi czy z sieci lokalnej. Aby uzyskać szczegółowe instrukcje, zobacz „Agent dla VMware — tworzenie kopii zapasowych bez obciążania sieci lokalnej” (s. 132).
- Rejestrowanie już zainstalowanego agenta dla VMware (s. 27)

  Z tej metody należy skorzystać, jeśli ręcznie zainstalowano agenta dla VMware (Windows), wdrożono agenta for VMware (urządzenie wirtualne) z szablonu OVF (s. 29) lub było konieczne ponowne zainstalowanie serwera zarządzania.

Wdrażanie agenta dla VMware (urządzenie wirtualne) przy użyciu interfejsu internetowego

1. Kliknij **Wszystkie urządzenia** > **Dodaj**.
2. Kliknij **VMware ESXi**.
3. Wybierz **Wdróż jako urządzenie wirtualne na każdym hoście serwera vCenter**.
4. Określ adres i poświadczenia dostępu dla serwera vCenter lub autonomicznego hosta ESXi. Zalecamy korzystanie z konta, które ma przypisaną rolę **Administrator**. W innym przypadku należy zadbać o dostęp do konta mającego niezbędne uprawnienia (s. 135) na serwerze vCenter lub ESXi.
5. [Opcjonalnie] Kliknij **Ustawienia**, aby dostosować ustawienia wdrożenia, takie jak:
   - Hosty ESXi, na których chcesz wdrożyć agenta (tylko wtedy, gdy w poprzednim kroku został określony serwer vCenter).
   - Nazwa urządzenia wirtualnego.
   - Magazyn danych, w którym będzie się znajdować urządzenie.
   - Pula zasobów lub obiekt vApp, które będą zawierać urządzenie.
   - Sieć, do której zostanie podłączona karta sieciowa urządzenia wirtualnego.

Copyright © Acronis International GmbH, 2002-2017

- Ustawienia sieciowe urządzenia wirtualnego. Możesz wybrać automatyczną konfigurację DHCP lub ręcznie określić poszczególne wartości, w tym statyczny adres IP.

6. Kliknij **Wdróż**.

Instalowanie agenta dla VMware (Windows)

Przygotowanie

Wykonaj czynności przygotowawcze opisane w sekcji „Dodawanie komputera z systemem Windows” (s. 24).

Instalacja

1. Kliknij **Wszystkie urządzenia** > **Dodaj**.
2. Kliknij **VMware ESXi**.
3. Wybierz **Zainstaluj zdalnie na komputerze z systemem Windows**.
4. Określ nazwę hosta lub adres IP komputera oraz poświadczenia znajdującego się na tym komputerze konta z uprawnieniami administracyjnymi. Kliknij **Połącz**.
5. Określ adres i poświadczenia dla serwera vCenter lub autonomicznego hosta ESXi, a następnie kliknij **Połącz**. Zalecamy korzystanie z konta, które ma przypisaną rolę **Administrator**. W innym przypadku należy zadbać o dostęp do konta mającego niezbędne uprawnienia (s. 135) na serwerze vCenter lub ESXi.
6. Kliknij **Zainstaluj**, aby zainstalować agenta.

Rejestrowanie już zainstalowanego agenta dla VMware

W tej sekcji opisano rejestrowanie agenta dla VMware przy użyciu interfejsu internetowego.

Alternatywne metody rejestracji:

- Agenta dla VMware (urządzenie wirtualne) można zarejestrować przez określenie serwera zarządzania w interfejsie użytkownika urządzenia wirtualnego. Zobacz krok 3 procedury „Konfigurowanie urządzenia wirtualnego” w sekcji „Wdrażanie agenta dla VMware (urządzenie wirtualne) przy użyciu szablonu OVF” (s. 29).
- Agent dla VMware (Windows) jest rejestrowany podczas instalacji lokalnej (s. 28).

Aby zarejestrować agenta dla VMware

1. Kliknij **Wszystkie urządzenia** > **Dodaj**.
2. Kliknij **VMware ESXi**.
3. Wybierz **Zarejestruj już zainstalowanego agenta**.
4. Jeśli rejestrujesz *agenta dla VMware (Windows)*, określ nazwę hosta lub adres IP komputera, na którym ten agent jest zainstalowany, i podaj poświadczenia znajdującego się na tym komputerze konta z uprawnieniami administracyjnymi.

   Jeśli rejestrujesz *agenta dla VMware (urządzenie wirtualne)*, określ nazwę hosta lub adres IP urządzenia wirtualnego i podaj poświadczenia dla serwera vCenter lub autonomicznego hosta ESXi, na którym to urządzenie działa.

   Kliknij **Połącz**.
5. Określ nazwę hosta lub adres IP serwera vCenter lub autonomicznego hosta ESXi, a także poświadczenia umożliwiające uzyskanie do niego dostępu, a następnie kliknij **Połącz**. Zalecamy korzystanie z konta, które ma przypisaną rolę **Administrator**. W innym przypadku należy zadbać o dostęp do konta mającego niezbędne uprawnienia (s. 135) na serwerze vCenter lub ESXi.
6. Kliknij **Zarejestruj**, aby zarejestrować agenta.

Copyright © Acronis International GmbH, 2002-2017

2.6.3 Instalowanie agentów lokalnie

2.6.3.1 Instalacja w systemie Windows

Aby zainstalować agenta dla systemu Windows, agenta dla Hyper-V, agenta dla programu Exchange, agenta dla SQL lub agenta dla usługi Active Directory

1. Zaloguj się jako administrator i uruchom program instalacyjny produktu Acronis Backup.
2. [Opcjonalnie] Aby zmienić język, w którym jest wyświetlany program instalacyjny, kliknij **Skonfiguruj język**.
3. Zaakceptuj warunki umowy licencyjnej i określ, czy komputer ma zostać objęty programem jakości obsługi klienta firmy Acronis.
4. Wybierz **Zainstaluj agenta kopii zapasowych**, a następnie określ nazwę hosta i adres IP komputera, na którym jest zainstalowany serwer zarządzania.

   Domyślnie zostaną zainstalowane następujące komponenty:

   - Agent dla systemu Windows
   - Inne agenty (agent dla Hyper-V, agent dla programu Exchange, agent dla SQL oraz agent dla usługi Active Directory), jeśli na komputerze zostaną wykryte odpowiedni hiperwizor lub odpowiednia aplikacja
   - Generator nośnika startowego
   - Narzędzie wiersza polecenia
   - Monitor kopii zapasowych

   Możesz skonfigurować instalację, klikając **Dostosuj ustawienia instalacji**.
5. Kontynuuj instalację.
6. Po zakończeniu instalacji kliknij **Zamknij**.

Aby zainstalować agenta dla VMware (Windows) lub agenta dla usługi Office 365

1. Zaloguj się jako administrator i uruchom program instalacyjny produktu Acronis Backup.
2. [Opcjonalnie] Aby zmienić język, w którym jest wyświetlany program instalacyjny, kliknij **Skonfiguruj język**.
3. Zaakceptuj warunki umowy licencyjnej i określ, czy komputer ma zostać objęty programem jakości obsługi klienta firmy Acronis.
4. Kliknij **Dostosuj ustawienia instalacji**.
5. Obok pozycji **Elementy do zainstalowania** kliknij **Zmień**.
6. Zaznacz pole wyboru **Agent dla VMware (Windows)** lub **Agent dla usługi Office 365**. Jeśli nie chcesz instalować na komputerze innych komponentów, usuń zaznaczenia odpowiednich pól wyboru. Kliknij **Gotowe**, aby kontynuować.
7. Obok pozycji **Acronis Backup Management Server** kliknij **Zmień**, a następnie określ nazwę hosta lub adres IP komputera, na którym jest zainstalowany serwer zarządzania. Kliknij **Gotowe**, aby kontynuować.
8. [Opcjonalnie] Zmień inne ustawienia instalacji.
9. Kliknij **Zainstaluj**, aby kontynuować instalację.
10. Po zakończeniu instalacji kliknij **Zamknij**.
11. [Tylko w przypadku instalacji agenta dla VMware (Windows)] Wykonaj procedurę opisaną w sekcji „Rejestrowanie już zainstalowanego agenta dla VMware” (s. 27).

Copyright © Acronis International GmbH, 2002-2017

2.6.3.2 Instalacja w systemie Linux

Przygotowanie

1. Przed zainstalowaniem programu w systemie, który nie używa menedżera RPM Package Manager, np. Ubuntu, należy ręcznie zainstalować ten menedżer (jako użytkownik root), na przykład przy użyciu następującego polecenia: **`apt-get install rpm`**.
2. Upewnij się, że na komputerze są zainstalowane niezbędne pakiety systemu Linux (s. 17).

Instalacja

Aby zainstalować agenta dla systemu Linux

1. Uruchom odpowiedni plik instalacyjny (.i686 lub .x86_64) jako użytkownik root.
2. Zaakceptuj warunki umowy licencyjnej.
3. Usuń zaznaczenie pola wyboru **Acronis Backup Management Server**, a następnie kliknij **Dalej**.
4. Określ nazwę hosta lub adresIP komputera, na którym jest zainstalowany serwer zarządzania.
5. Kliknij **Dalej**, aby kontynuować instalację.
6. Po zakończeniu instalacji kliknij **Wyjście**.

Informacje dotyczące rozwiązywania problemów są dostępne w pliku:
/usr/lib/Acronis/BackupAndRecovery/HOWTO.INSTALL

2.6.3.3 Instalacja w systemie OS X

Aby zainstalować agenta dla systemu Mac

1. Kliknij dwukrotnie plik instalacyjny (.dmg).
2. Poczekaj, aż system operacyjny zamontuje instalacyjny obraz dysku.
3. Kliknij dwukrotnie **Zainstaluj**.
4. Postępuj zgodnie z instrukcjami wyświetlanymi na ekranie.

2.6.3.4 Wdrażanie agenta dla VMware (urządzenie wirtualne) przy użyciu szablonu OVF

Gdy serwer zarządzania zostanie już zainstalowany, pakiet OVF urządzenia wirtualnego będzie się znajdować w folderze **%ProgramFiles%\Acronis\ESXAppliance** (w systemie Windows) lub **/usr/lib/Acronis/ESXAppliance** (w systemie Linux).

Folder ten zawiera jeden plik .ovf i dwa pliki .vmdk. Dopilnuj, aby do tych plików można było uzyskać dostęp z komputera z klientem vSphere.

Wdrażanie szablonu OVF

1. Uruchom klienta vSphere i zaloguj się na serwerze vCenter.
2. W menu **File** (Plik) kliknij **Deploy OVF Template** (Wdróż szablon OVF).
3. Na stronie **Source** (Źródło) określ ścieżkę do pakietu OVF urządzenia wirtualnego.
4. Przejrzyj informacje w sekcji **OVF Template Details** (Informacje o szablonie OVF) i kliknij **Next** (Dalej).
5. Na stronie **Name and Location** (Nazwa i lokalizacja) wpisz nazwę urządzenia lub pozostaw nazwę domyślną **AcronisESXAppliance**.
6. W polu **Host / Cluster** (Host/klaster) wybierz host ESXi, na którym zostanie wdrożone urządzenie.
7. [Opcjonalnie] W polu **Resource Pool** (Pula zasobów) wybierz pulę zasobów zawierającą dane urządzenie.

Copyright © Acronis International GmbH, 2002-2017

8. W polu **Storage** (Magazyn) pozostaw wybrany domyślny magazyn danych, chyba że jest w nim za mało miejsca na urządzenie wirtualne. W takim przypadku wybierz inny magazyn danych. Jeśli na serwerze jest tylko jeden magazyn danych, pomiń ten krok.
9. W polu **Disk Format** (Format dysku) wybierz wymaganą wartość. Format dysku nie ma wpływu na wydajność urządzenia.
10. Na stronie **Network mapping** (Mapowanie sieci) wybierz tryb mostka dla karty sieciowej.
11. Przejrzyj podsumowanie i kliknij **Finish** (Zakończ). Po wyświetleniu raportu o pomyślnym zakończeniu wdrażania zamknij okno postępu.

Konfigurowanie urządzenia wirtualnego

1. **Uruchamianie urządzenia wirtualnego**

   W kliencie vSphere przejdź do ekranu **Inventory** (Inwentaryzacja), kliknij prawym przyciskiem myszy nazwę urządzenia wirtualnego, a następnie kliknij **Power** (Zasilanie) > **Power On** (Włącz). Wybierz kartę **Console** (Konsola). Na ekranie powitalnym kliknij **Close** (Zamknij).

2. **vCenter/ESX(i)**

   W obszarze **Opcje agenta**, w polu **vCenter/ESX(i)** kliknij **Zmień** i określ nazwę lub adres IP serwera vCenter. Agent będzie mógł tworzyć kopie zapasowe i odzyskiwać wszystkie maszyny wirtualne zarządzane przez serwer vCenter.

   Jeśli nie używasz serwera vCenter, określ nazwę lub adres IP hosta ESXi z maszynami wirtualnymi, których kopie zapasowe chcesz tworzyć i odzyskiwać. Zwykle tworzenie kopii zapasowych maszyn wirtualnych przez agenta znajdującego się na tym samym hoście przebiega szybciej.

   Określ poświadczenia, których będzie używał agent do łączenia się z serwerem vCenter lub ESXi. Zalecamy korzystanie z konta, które ma przypisaną rolę **Administrator**. W innym przypadku należy zadbać o dostęp do konta mającego niezbędne uprawnienia (s. 135) na serwerze vCenter lub ESXi.

   Aby upewnić się, że poświadczenia dostępu są poprawne, możesz kliknąć **Sprawdź połączenie**.

3. **Acronis Backup Management Server**

   W obszarze **Opcje agenta**, w polu **Acronis Backup Management Server** kliknij **Zmień**.

   Określ nazwę hosta lub adres IP komputera, na którym jest zainstalowany serwer zarządzania, a następnie poświadczenia dostępu dla tego komputera.

4. **Strefa czasowa**

   W obszarze **Maszyna wirtualna**, w polu **Strefa czasowa** kliknij **Zmień**. Wybierz strefę czasową swojej lokalizacji, aby się upewnić, że zaplanowane operacje zostaną uruchomione w odpowiednim czasie.

Urządzenie wirtualne jest gotowe do pracy. Ponadto możesz zmienić następujące ustawienia:

- **Ustawienia sieciowe**

  Połączenie sieciowe agenta jest konfigurowane automatycznie przy użyciu protokołu DHCP (Dynamic Host Configuration Protocol). Aby zmienić konfigurację domyślną, w sekcji **Opcje agenta** w polu **eth0** kliknij **Zmień** i określ żądane ustawienia sieciowe.

- **Magazyny lokalne**

  Do urządzenia wirtualnego można podłączyć dodatkowy dysk, tak aby agent dla VMware mógł tworzyć kopie zapasowe w takim dołączonym lokalnie magazynie. Tego rodzaju konfiguracja zwykle zapewnia szybsze tworzenie kopii zapasowych niż przez sieć lokalną i nie zajmuje całej przepustowości sieci.

  Dysk wirtualny nie może być mniejszy niż 10 GB. Dodaj dysk, edytując ustawienia maszyny wirtualnej, i kliknij **Odśwież**. Łącze **Utwórz magazyn** stanie się dostępne. Kliknij je, wybierz dysk i określ jego etykietę.

Copyright © Acronis International GmbH, 2002-2017

Dodając już istniejący dysk, zachowaj ostrożność. Po utworzeniu magazynu wszystkie dane zawarte dotychczas na tym dysku zostaną utracone.

2.6.4 Zarządzanie licencjami

Licencjonowanie programu Acronis Backup opiera się na liczbie komputerów fizycznych oraz hostów wirtualizacji uwzględnianych w kopiach zapasowych. Można korzystać z zarówno licencji subskrypcyjnych, jak i licencji wieczystych. Okres wygasania subskrypcji rozpoczyna się w chwili rejestracji w witrynie internetowej firmy Acronis.

Aby zacząć korzystać z programu Acronis Backup, trzeba dodać do serwera zarządzania co najmniej jeden klucz licencyjny. Licencja jest automatycznie przypisywana do komputera po zastosowaniu planu tworzenia kopii zapasowych. Licencje można też przypisywać i odwoływać ręcznie.

Aby dodać klucz licencyjny

1. Kliknij **Ustawienia** > **Licencje**.
2. Kliknij **Dodaj klucze**.
3. Wprowadź klucze licencyjne.
4. Kliknij **Dodaj**.
5. Aby aktywować subskrypcję, trzeba się zalogować. Jeśli został wprowadzony choć jeden klucz subskrypcji, wprowadź adres e-mail i hasło konta Acronis, a następnie kliknij **Zaloguj się**. Jeśli zostały wprowadzone tylko klucze wieczyste, pomiń ten krok.
6. Kliknij **Gotowe**.

Wskazówka *Jeśli klucze subskrypcji są już zarejestrowane, serwer zarządzania może je zaimportować z konta Acronis. Aby zsynchronizować klucze subskrypcji, kliknij* ***Synchronizuj*** *i zaloguj się.*

Zarządzanie licencjami wieczystymi

Aby przypisać licencję wieczystą do komputera

1. Kliknij **Ustawienia** > **Licencje**.
2. Wybierz licencję wieczystą.

   Oprogramowanie wyświetli klucze licencyjne odpowiadające wybranej licencji.
3. Wybierz klucz do przypisania.
4. Kliknij **Przypisz**.

   Oprogramowanie wyświetli komputery, do których można przypisać wybrany klucz.
5. Wybierz komputer i kliknij **Gotowe**.

Aby odwołać licencję wieczystą z komputera

1. Kliknij **Ustawienia** > **Licencje**.
2. Wybierz licencję wieczystą.

   Oprogramowanie wyświetli klucze licencyjne odpowiadające wybranej licencji. Komputer, do którego został przypisany klucz, jest widoczny w kolumnie **Przypisano do**.
3. Wybierz klucz licencyjny do odwołania.
4. Kliknij **Odwołaj**.
5. Potwierdź decyzję.

   Odwołany klucz pozostanie na liście kluczy licencyjnych. Można go przypisać do innego komputera.

Copyright © Acronis International GmbH, 2002-2017

Zarządzanie licencjami subskrypcyjnymi

Aby przypisać licencję subskrypcyjną do komputera

1. Kliknij **Ustawienia** > **Licencje**.
2. Wybierz licencję subskrypcyjną.
   Oprogramowanie wyświetli komputery, do których wybrana licencja jest już przypisana.
3. Kliknij **Przypisz**.
   Oprogramowanie wyświetli komputery, do których można przypisać wybraną licencję.
4. Wybierz komputer i kliknij **Gotowe**.

Aby odwołać licencję subskrypcyjną z komputera

1. Kliknij **Ustawienia** > **Licencje**.
2. Wybierz licencję subskrypcyjną.
   Oprogramowanie wyświetli komputery, do których wybrana licencja jest już przypisana.
3. Wybierz komputer, z którego chcesz odwołać licencję.
4. Kliknij **Odwołaj licencję**.
5. Potwierdź decyzję.

2.7 Wdrożenie chmurowe

2.7.1 Przygotowanie

Krok 1

Wybierz agenta w zależności od elementów, których kopię zapasową chcesz utworzyć. Aby uzyskać informacje na temat agentów, zobacz sekcję „Komponenty” (s. 9).

Krok 2

Pobierz program instalacyjny. Aby znaleźć łącza pobierania, kliknij **Wszystkie urządzenia** > **Dodaj**.

Na stronie **Dodaj urządzenia** są dostępne instalatory internetowe każdego agenta instalowanego w systemie Windows. Instalator internetowy jest małym plikiem wykonywalnym, który pobiera główny program instalacyjny z Internetu i zapisuje go jako plik tymczasowy. Plik ten jest usuwany natychmiast po zakończeniu instalacji.

Jeśli chcesz przechowywać programy instalacyjne lokalnie, pobierz pakiet zawierający wszystkie agenty do instalacji w systemie Windows, korzystając z łącza dostępnego u dołu strony **Dodaj urządzenia**. Pakiet jest dostępny w wersji zarówno 32-, jak i 64-bitowej. Pakiety te umożliwiają dostosowanie listy komponentów do zainstalowania. Pakiet umożliwia instalację nienadzorowaną, na przykład przy użyciu zasad grupy. Ten zaawansowany scenariusz został opisany w sekcji „Wdrażanie agentów przy użyciu zasad grupy” (s. 36).

W systemach Linux i OS X instalację wykonuje się przy użyciu zwykłych programów instalacyjnych.

Wszystkie te programy instalacyjne wymagają połączenia z Internetem w celu rejestracji komputera w usłudze tworzenia kopii zapasowych. W przypadku braku połączenia z Internetem instalacja się nie powiedzie.

Copyright © Acronis International GmbH, 2002-2017

Krok 3

Przed instalacją upewnij się, że zapory i inne komponenty systemu zabezpieczeń sieci (np. serwer proxy) umożliwiają połączenia — zarówno przychodzące, jak i wychodzące — przez następujące porty TCP:

- **443** i **8443**. Porty te służą do uzyskiwania dostępu do konsoli kopii zapasowych, rejestrowania agentów, pobierania certyfikatów, autoryzacji użytkowników oraz pobierania plików z chmury.
- **7770...7800** Agenty używają tych portów do komunikacji z serwerem zarządzania kopiami zapasowymi.
- **44445** Agenty używają tego portu do przesyłania danych podczas tworzenia kopii zapasowych i odzyskiwania.

Jeśli w danej sieci jest włączony serwer proxy, zajrzyj do sekcji „Ustawienia serwera proxy” (s. 33), aby sprawdzić, czy trzeba skonfigurować te ustawienia na każdym komputerze z uruchomionym agentem kopii zapasowych.

2.7.2 Ustawienia serwera proxy

Agenty kopii zapasowych mogą przesyłać dane przez serwer proxy HTTP.

Do instalacji agenta wymagane jest połączenie z Internetem. Jeśli w systemie Windows jest skonfigurowany serwer proxy (**Panel sterowania** > **Opcje internetowe** > **Połączenia**), program instalacyjny automatycznie odczyta ustawienia serwera proxy z rejestru i ich użyje. W systemach Linux i OS X trzeba określić ustawienia serwera proxy przed instalacją.

Aby określić ustawienia serwera proxy przed instalacją agenta lub zmienić je w późniejszym czasie, skorzystaj z poniższych procedur.

W systemie Linux

1. Utwórz plik **/etc/Acronis/Global.config** i otwórz go w edytorze tekstów.
2. Skopiuj i wklej do pliku następujące wiersze:

```
<?xml version="1.0" ?>
<registry name="Global">
    <key name="HttpProxy">
        <value name="Enabled" type="Tdword">"1"</value>
        <value name="Host" type="TString">"proxy.company.com"</value>
        <value name="Port" type="Tdword">"443"</value>
    </key>
</registry>
```

3. Zastąp `proxy.company.com` nazwą hosta / adresem IP serwera proxy, a `443` — wartością dziesiętną numeru portu.
4. Zapisz plik.
5. Jeśli agent kopii zapasowych nie jest jeszcze zainstalowany, możesz go teraz zainstalować. W przeciwnym wypadku uruchom ponownie agenta, wykonując w dowolnym katalogu następujące polecenie:

```
sudo service acronis_mms restart
```

W systemie OS X

1. Utwórz plik **/Library/Application Support/Acronis/Registry/Global.config** i otwórz go w edytorze tekstów, np. w programie Text Edit.
2. Skopiuj i wklej do pliku następujące wiersze:

Copyright © Acronis International GmbH, 2002-2017

```
<?xml version="1.0" ?>
<registry name="Global">
    <key name="HttpProxy">
        <value name="Enabled" type="Tdword">"1"</value>
        <value name="Host" type="TString">"proxy.company.com"</value>
        <value name="Port" type="Tdword">"443"</value>
    </key>
</registry>
```

3. Zastąp `proxy.company.com` nazwą hosta / adresem IP serwera proxy, a `443` — wartością dziesiętną numeru portu.
4. Zapisz plik.
5. Jeśli agent kopii zapasowych nie jest jeszcze zainstalowany, możesz go teraz zainstalować. W przeciwnym wypadku uruchom ponownie agenta, wykonując następujące czynności:
   a. Przejdź do sekcji **Aplikacje** > **Narzędzia** > **Terminal**.
   b. Uruchom następujące polecenia:

```
sudo launchctl stop acronis_mms
sudo launchctl start acronis_mms
```

W systemie Windows

1. Utwórz nowy dokument tekstowy i otwórz go w edytorze tekstów, np. w programie Notatnik.
2. Skopiuj i wklej do pliku następujące wiersze:

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\Global\HttpProxy]
"Enabled"=dword:00000001
"Host"="proxy.company.com"
"Port"=dword:000001bb
```

3. Zastąp `proxy.company.com` nazwą hosta / adresem IP serwera proxy, a `000001bb` — wartością szesnastkową numeru portu. Na przykład wartość `000001bb` oznacza port 443.
4. Zapisz dokument pod nazwą **proxy.reg**.
5. Uruchom plik jako administrator.
6. Potwierdź, że chcesz edytować rejestr systemu Windows.
7. Jeśli agent kopii zapasowych nie jest jeszcze zainstalowany, możesz go teraz zainstalować. W przeciwnym wypadku uruchom ponownie agenta, wykonując następujące czynności:
   a. W menu **Start** kliknij **Uruchom**, a następnie wpisz: **cmd**.
   b. Kliknij **OK**.
   c. Uruchom następujące polecenia:

```
net stop mms
net start mms
```

2.7.3 Instalowanie agentów

W systemie Windows

1. Upewnij się, że komputer ma połączenie z Internetem.
2. Zaloguj się jako administrator i uruchom program instalacyjny.
3. Kliknij **Zainstaluj**.
4. Określ poświadczenia konta, do którego powinien zostać przypisany dany komputer.

Copyright © Acronis International GmbH, 2002-2017

5. Jeśli chcesz zweryfikować lub zmienić nazwę hosta / adres IP oraz port serwera proxy, kliknij **Pokaż ustawienia serwera proxy**. W przeciwnym razie pomiń ten krok. W przypadku włączenia serwera proxy w systemie Windows zostanie on automatycznie wykryty i użyty.
6. [Tylko w przypadku instalowania agenta dla VMware] Określ adres i poświadczenia dostępu serwera vCenter lub autonomicznego hosta ESXi, którego maszyny wirtualne agent uwzględni w kopii zapasowej. Zalecamy korzystanie z konta, które ma przypisaną rolę **Administrator**. W innym przypadku należy zadbać o dostęp do konta mającego niezbędne uprawnienia (s. 135) na serwerze vCenter lub ESXi.
7. [Tylko w przypadku instalowania na kontrolerze domeny] Określ konto użytkownika, które będzie służyć do uruchamiania usługi agenta. Ze względów bezpieczeństwa program instalacyjny nie tworzy automatycznie nowych kont na kontrolerze domeny.
8. Kliknij **Rozpocznij instalację**.

Możesz zmienić ścieżkę instalacji oraz konto usługi agenta. W tym celu kliknij **Dostosuj ustawienia instalacji** w pierwszym kroku kreatora instalacji.

W systemie Linux

1. Upewnij się, że komputer ma połączenie z Internetem.
2. Uruchom plik instalacyjny jako użytkownik root.
3. Określ poświadczenia konta, do którego powinien zostać przypisany dany komputer.
4. Zaznacz pola wyboru odpowiadające agentom, które chcesz zainstalować. Dostępne są następujące agenty:
   - **Agent dla systemu Linux**
   - **Agent dla Virtuozzo**

   Agenta dla Virtuozzo nie można zainstalować bez agenta dla systemu Linux.
5. Wykonaj procedurę instalacji.

Informacje dotyczące rozwiązywania problemów są dostępne w pliku:
/usr/lib/Acronis/BackupAndRecovery/HOWTO.INSTALL

W systemie OS X

1. Upewnij się, że komputer ma połączenie z Internetem.
2. Kliknij dwukrotnie plik instalacyjny (.dmg).
3. Poczekaj, aż system operacyjny zamontuje instalacyjny obraz dysku.
4. Kliknij dwukrotnie **Zainstaluj**.
5. Jeśli pojawi się monit, podaj poświadczenia administratora.
6. Określ poświadczenia konta, do którego powinien zostać przypisany dany komputer.
7. Wykonaj procedurę instalacji.

2.7.4 Aktywacja konta

Gdy administrator utworzy Twoje konto, na Twój adres e-mail zostanie wysłana wiadomość. Wiadomość ta zawiera następujące informacje:

- **Łącze aktywacji konta.** Kliknij to łącze i ustaw hasło konta. Zapamiętaj nazwę logowania widoczną na stronie aktywacji konta.
- **Łącze do strony logowania do konsoli kopii zapasowych.** Za pomocą tego łącza można uzyskiwać dostęp do konsoli w przyszłości. Nazwa logowania i hasło są takie same jak te, które zostały użyte w poprzednim kroku.

Copyright © Acronis International GmbH, 2002-2017

2.8 Wdrażanie agentów przy użyciu zasad grupy

Agenta dla systemu Windows można centralnie zainstalować (lub wdrożyć) na komputerach należących do domeny Active Directory, korzystając z zasad grupy.

W tej sekcji przedstawiono sposób konfigurowania obiektu zasad grupy w celu wdrożenia agentów na komputerach w całej domenie lub jej jednostce organizacyjnej.

Za każdym razem, gdy komputer loguje się do domeny, wynikowy obiekt zasad grupy sprawdza, czy agent jest zainstalowany i zarejestrowany.

Wymagania wstępne

Przed rozpoczęciem wdrażania agenta upewnij się, że:

- Istnieje domena Active Directory z kontrolerem domeny, na którym działa system Microsoft Windows Server 2003 lub nowszy.
- Należysz do grupy **Administratorzy domeny** w domenie.
- Masz pobrany program instalacyjny **Wszystkie agenty do instalacji w systemie Windows**. Łącze pobierania jest dostępne na stronie **Dodaj urządzenia** konsoli kopii zapasowych.

Krok 1: Tworzenie transformacji .mst i wyodrębnianie pakietu instalacyjnego

1. Zaloguj się jako administrator na dowolnym komputerze w domenie.
2. Utwórz folder udostępniony, w którym będą przechowywane pakiety instalacyjne. Upewnij się, że użytkownicy domeny mają dostęp do tego folderu udostępnionego — w tym celu na przykład pozostaw domyślne ustawienia udostępniania dla opcji **Wszyscy**.
3. Skopiuj program instalacyjny do utworzonego folderu.
4. Uruchom program instalacyjny.
5. Kliknij **Utwórz pliki .mst i .msi na potrzeby instalacji nienadzorowanej**.
6. Jeśli pojawi się stosowny monit, określ poświadczenia konta, do którego powinny zostać przypisane komputery.
7. Przejrzyj lub zmodyfikuj ustawienia instalacji, które zostaną dodane do pliku .mst.
8. Kliknij **Generuj**.

W wyniku tego zostanie wygenerowana transformacja .mst, a do utworzonego folderu zostaną wyodrębnione pakiety instalacyjne .msi oraz .cab. Teraz możesz przenieść lub usunąć plik .exe programu instalacyjnego.

Krok 2: Konfigurowanie obiektów zasad grupy

1. Zaloguj się na kontrolerze domeny jako administrator domeny. Jeśli domena ma więcej niż jeden kontroler, zaloguj się na dowolnym z nich jako administrator domeny.
2. Planując wdrożenie agenta w jednostce organizacyjnej, upewnij się, że ta jednostka istnieje w domenie. W przeciwnym razie pomiń ten krok.
3. W menu **Start** wskaż **Narzędzia administracyjne**, a następnie kliknij **Użytkownicy i komputery usługi Active Directory** (w systemie Windows Server 2003) lub **Zarządzanie zasadami grupy** (w systemach Windows Server 2008 i Windows Server 2012).
4. W systemie Windows Server 2003:
   - Kliknij prawym przyciskiem myszy domenę lub jednostkę organizacyjną, a następnie kliknij **Właściwości**. W oknie dialogowym kliknij kartę **Zasady grupy**, a następnie kliknij **Nowy**.

   W systemach Windows Server 2008 i Windows Server 2012:

Copyright © Acronis International GmbH, 2002-2017

- Kliknij prawym przyciskiem myszy nazwę domeny lub jednostki organizacyjnej, a następnie kliknij **Utwórz obiekt zasad grupy w tej domenie i umieść tu łącze**.

5. Nadaj nazwę nowemu obiektowi zasad grupy **Agent dla systemu Windows**.
6. Otwórz obiekt zasad grupy **Agent dla systemu Windows** do edycji w następujący sposób:
   - W systemie Windows Server 2003 kliknij ten obiekt zasad grupy, a następnie kliknij **Edytuj**.
   - W systemach Windows Server 2008 i Windows Server 2012 w obszarze **Obiekty zasad grupy** kliknij prawym przyciskiem myszy ten obiekt zasad grupy, a następnie kliknij **Edytuj**.
7. W przystawce Edytor obiektów zasad grupy rozwiń węzeł **Konfiguracja komputera**.
8. W systemach Windows Server 2003 i Windows Server 2008:
   - Rozwiń węzeł **Ustawienia oprogramowania**.

   W systemie Windows Server 2012:
   - Rozwiń **Zasady** > **Ustawienia oprogramowania**.
9. Kliknij prawym przyciskiem myszy **Instalacja oprogramowania**, wskaż **Nowy**, a następnie kliknij **Pakiet**.
10. Wybierz pakiet instalacyjny .msi agenta we wcześniej utworzonym folderze udostępnionym, a następnie kliknij **Otwórz**.
11. W oknie dialogowym **Rozmieszczanie oprogramowania** kliknij **Zaawansowane**, a następnie kliknij **OK**.
12. Na karcie **Modyfikacje** kliknij **Dodaj**, a następnie wybierz wcześniej utworzoną transformację .mst.
13. Kliknij **OK**, aby zamknąć okno dialogowe **Rozmieszczanie oprogramowania**.

2.9 Aktualizowanie agentów

- Wdrożenie lokalne: w celu zaktualizowania agentów należy najpierw zaktualizować serwer zarządzania, a następnie powtórzyć instalację agenta lokalnie lub przy użyciu interfejsu internetowego.
- Wdrożenie chmurowe: agenty są aktualizowane automatycznie, gdy tylko zostanie wydana nowa wersja. Jeśli aktualizacja automatyczna z jakiegoś powodu się nie powiedzie, skorzystaj z procedury opisanej poniżej.

Aby sprawdzić wersję agenta, wybierz komputer i kliknij **Przegląd**.

Aby zaktualizować agenta we wdrożeniu chmurowym

1. Kliknij **Ustawienia** > **Agenty**.

   W oprogramowaniu zostanie wyświetlona lista komputerów. Komputery z nieaktualnymi wersjami agentów są oznaczone pomarańczowym wykrzyknikiem.
2. Wybierz komputery, na których chcesz zaktualizować agenty. Komputery te muszą być w trybie online.
3. Kliknij **Aktualizuj agenta**.

   Postęp aktualizacji jest widoczny w kolumnie statusu każdego komputera.

2.10 Odinstalowywanie produktu

Jeśli chcesz usunąć z komputera poszczególne komponenty produktu, uruchom program instalacyjny, wybierz opcję modyfikacji produktu i usuń zaznaczenia komponentów do usunięcia. Łącza do programów instalacyjnych są dostępne na stronie **Downloads** (Materiały do pobrania) (kliknij ikonę konta w prawym górnym rogu > **Downloads**).

Copyright © Acronis International GmbH, 2002-2017

Jeśli chcesz usunąć z komputera wszystkie komponenty produktu, wykonaj czynności opisane poniżej.

Ostrzeżenie *W przypadku wdrożeń lokalnych dopilnuj, aby omyłkowo nie odinstalować serwera zarządzania. Konsola kopii zapasowych przestałaby być dostępna. Nie można by już było utworzyć kopii zapasowej ani odzyskać żadnego z komputerów zarejestrowanych na serwerze zarządzania.*

W systemie Windows

1. Zaloguj się jako administrator.
2. Przejdź do **Panelu sterowania**, a następnie wybierz **Programy i funkcje** (**Dodaj lub usuń programy** w systemie Windows XP) > **Acronis Backup** > **Odinstaluj**.
3. [Opcjonalnie] Zaznacz pole wyboru **Usuń dzienniki i ustawienia konfiguracji**.

   Pozostaw to pole niezaznaczone, jeśli odinstalowujesz agenta, ale planujesz go ponownie zainstalować. Jeśli zaznaczysz to pole wyboru, komputer zostanie zduplikowany w konsoli kopii zapasowych, a kopie zapasowe starego komputera nie zostaną powiązane z nowym komputerem.
4. Potwierdź decyzję.
5. Jeśli planujesz zainstalować agenta ponownie, pomiń ten krok. W przeciwnym razie w konsoli kopii zapasowych kliknij **Ustawienia** > **Agenty**, zaznacz komputer, na którym agent został zainstalowany, a następnie kliknij **Usuń**.

W systemie Linux

1. Jako użytkownik root uruchom polecenie **/usr/lib/Acronis/BackupAndRecovery/uninstall/uninstall**.
2. [Opcjonalnie] Zaznacz pole wyboru **Wyczyść wszystkie ślady produktu (usuń jego dzienniki, zadania, skarbce i ustawienia konfiguracji)**.

   Pozostaw to pole niezaznaczone, jeśli odinstalowujesz agenta, ale planujesz go ponownie zainstalować. Jeśli zaznaczysz to pole wyboru, komputer zostanie zduplikowany w konsoli kopii zapasowych, a kopie zapasowe starego komputera nie zostaną powiązane z nowym komputerem.
3. Potwierdź decyzję.
4. Jeśli planujesz zainstalować agenta ponownie, pomiń ten krok. W przeciwnym razie w konsoli kopii zapasowych kliknij **Ustawienia** > **Agenty**, zaznacz komputer, na którym agent został zainstalowany, a następnie kliknij **Usuń**.

W systemie OS X

1. Kliknij dwukrotnie plik instalacyjny (.dmg).
2. Poczekaj, aż system operacyjny zamontuje instalacyjny obraz dysku.
3. W obrazie kliknij dwukrotnie **Odinstaluj**.
4. Jeśli pojawi się monit, podaj poświadczenia administratora.
5. Potwierdź decyzję.
6. Jeśli planujesz zainstalować agenta ponownie, pomiń ten krok. W przeciwnym razie w konsoli kopii zapasowych kliknij **Ustawienia** > **Agenty**, zaznacz komputer, na którym agent został zainstalowany, a następnie kliknij **Usuń**.

Usuwanie agenta dla VMware (urządzenie wirtualne)

1. Uruchom klienta vSphere i zaloguj się na serwerze vCenter.
2. Jeśli urządzenie wirtualne jest włączone, kliknij je prawym przyciskiem myszy, a następnie kliknij **Zasilanie** > **Wyłącz**. Potwierdź decyzję.

Copyright © Acronis International GmbH, 2002-2017

3. Jeśli urządzenie wirtualne używa magazynu dołączonego lokalnie na dysku wirtualnym i chcesz zachować dane na tym dysku, wykonaj następujące czynności:
   a. Kliknij prawym przyciskiem myszy urządzenie wirtualne, a następnie kliknij **Edytuj ustawienia**.
   b. Wybierz dysk z magazynem i kliknij **Usuń**. W obszarze **Opcje usuwania** kliknij **Usuń z maszyny wirtualnej**.
   c. Kliknij **OK**.

   W wyniku tej operacji dysk pozostanie w magazynie danych. Dysk można dołączyć do innego urządzenia wirtualnego.
4. Kliknij prawym przyciskiem myszy urządzenie wirtualne, a następnie kliknij **Usuń z dysku**. Potwierdź decyzję.
5. Jeśli planujesz zainstalować agenta ponownie, pomiń ten krok. W przeciwnym razie w konsoli kopii zapasowych kliknij **Ustawienia** > **Agenty**, zaznacz urządzenie wirtualne, a następnie kliknij **Usuń**.

3 Dostęp do konsoli kopii zapasowych

W pasku adresu przeglądarki wprowadź adres strony logowania, a następnie określ nazwę użytkownika i hasło.

Wdrożenie lokalne

Adres strony logowania to adres IP lub nazwa komputera, na którym jest zainstalowany serwer zarządzania.

Aby móc się zalogować, musisz być członkiem grupy **Acronis Centralized Admins** (Administratorzy centralni) na komputerze, na którym działa serwer zarządzania. Domyślnie do tej grupy należą wszyscy członkowie grupy **Administratorzy**. Jeśli serwer zarządzania jest zainstalowany w systemie Linux, zalogować się może tylko użytkownik root.

Wdrożenie chmurowe

Adres strony logowania jest następujący: https://backup.acronis.com/. Nazwa użytkownika i hasło są takie same jak w przypadku konta Acronis.

Jeśli konto zostało utworzone przez administratora kopii zapasowych, należy je aktywować i ustawić hasło przez kliknięcie łącza w aktywacyjnej wiadomości e-mail.

Zmienianie języka

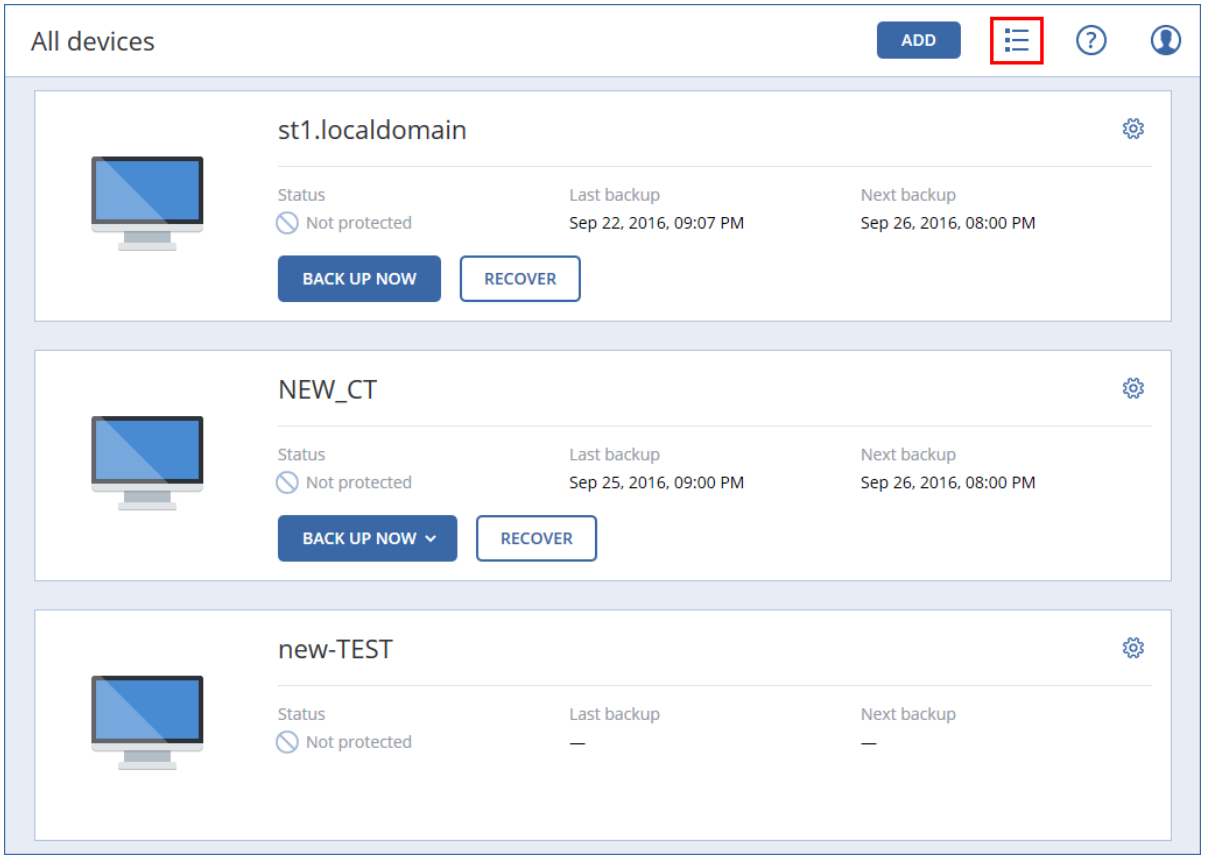
Po zalogowaniu się możesz zmienić język interfejsu internetowego, klikając ikonę z ludzką sylwetką w prawym górnym rogu.

4 Widoki konsoli kopii zapasowych

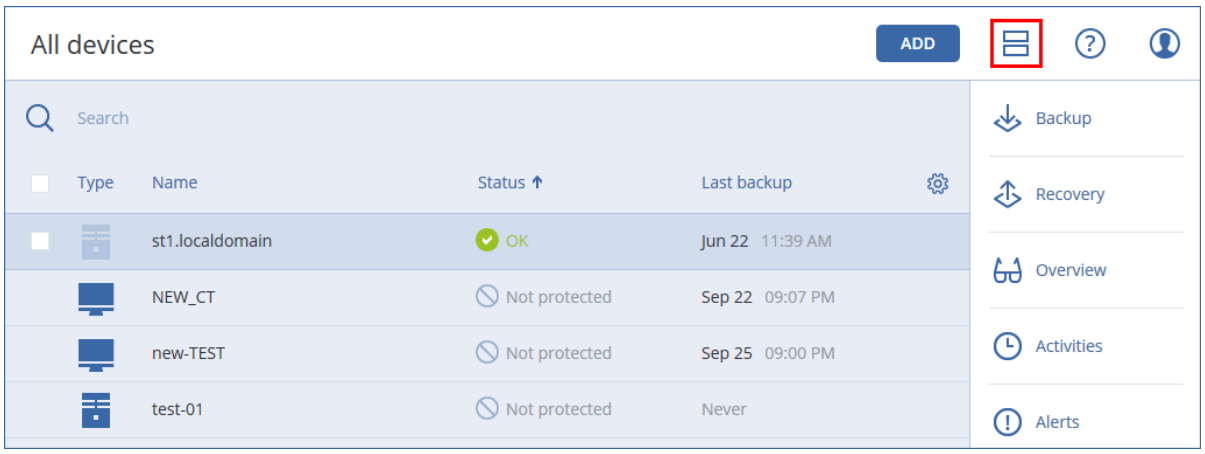
Konsola kopii zapasowych ma dwa widoki: widok prosty i widok tabeli. Aby przełączyć widok, kliknij odpowiednią ikonę w prawym górnym rogu.

Copyright © Acronis International GmbH, 2002-2017

Widok prosty obsługuje niewielką liczbę komputerów.



Widok tabeli jest włączany automatycznie, jeśli liczba komputerów będzie duża.



Oba widoki zapewniają dostęp do tych samych funkcji i operacji. W niniejszym dokumencie opisano dostęp do operacji z poziomu widoku tabeli.

5 Kopia zapasowa

Plan tworzenia kopii zapasowych to zestaw reguł określających sposób ochrony konkretnych danych na konkretnym komputerze.

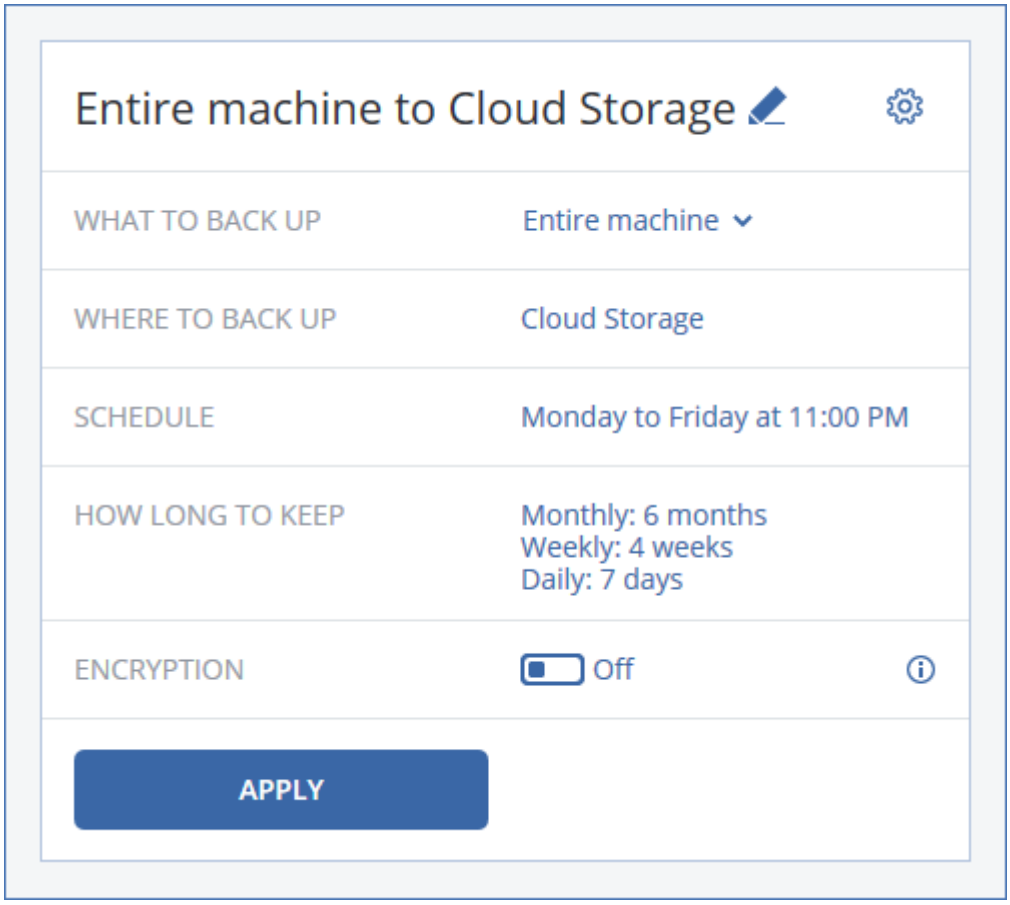
Plan tworzenia kopii zapasowych można zastosować do wielu komputerów — w trakcie jego tworzenia lub później.

Copyright © Acronis International GmbH, 2002-2017

Aby utworzyć pierwszy plan tworzenia kopii zapasowych

1. Wybierz komputery, których kopie zapasowe chcesz utworzyć.
2. Kliknij **Kopia zapasowa**.

   W oprogramowaniu zostanie wyświetlony nowy szablon planu tworzenia kopii zapasowych.



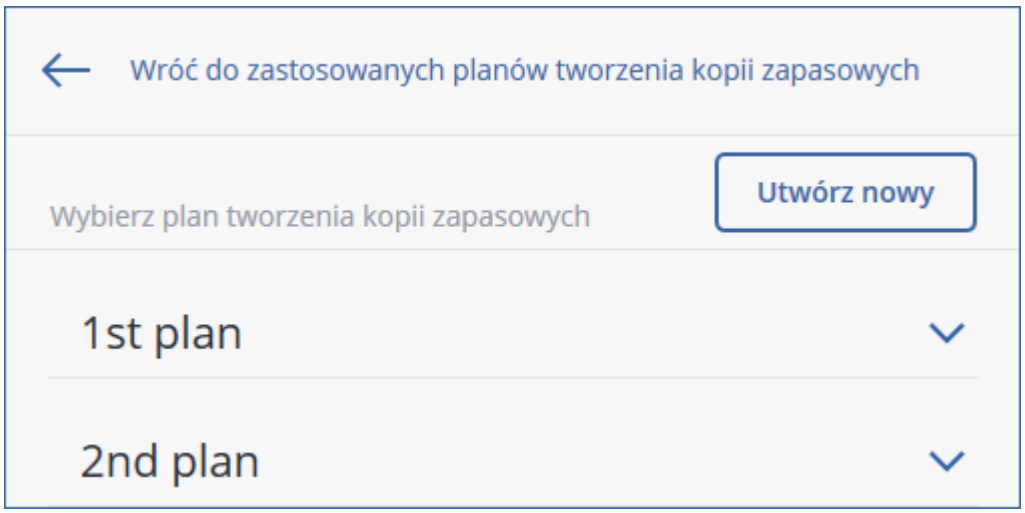
3. [Opcjonalnie] Aby zmodyfikować nazwę planu tworzenia kopii zapasowych, kliknij nazwę domyślną.
4. [Opcjonalnie] Aby zmodyfikować parametry planu tworzenia kopii zapasowych, kliknij odpowiednią sekcję w panelu planu.
5. [Opcjonalnie] Aby zmodyfikować opcje tworzenia kopii zapasowych, kliknij ikonę koła zębatego.
6. Kliknij **Zastosuj**.

Aby zastosować już istniejący plan tworzenia kopii zapasowych

1. Wybierz komputery, których kopie zapasowe chcesz utworzyć.
2. Kliknij **Kopia zapasowa**. Jeśli do wybranych komputerów jest już stosowany typowy plan tworzenia kopii zapasowych, kliknij **Dodaj plan tworzenia kopii zapasowych**.

Copyright © Acronis International GmbH, 2002-2017

W oprogramowaniu zostaną wyświetlone utworzone wcześniej plany tworzenia kopii zapasowych.



3. Wybierz plan tworzenia kopii zapasowych, który chcesz zastosować.
4. Kliknij **Zastosuj**.

5.1 Plan tworzenia kopii zapasowych — ściągawka

W poniższej tabeli zestawiono dostępne parametry planów tworzenia kopii zapasowych. Dzięki niej przygotujesz optymalny plan tworzenia kopii zapasowych.

OBIEKTY DO UWZGLĘDNIENIA W KOPII ZAPASOWEJ	**ELEMENTY DO UWZGLĘDNIENIA W KOPII ZAPASOWEJ** **Metody wyboru**	**MIEJSCE DOCELOWE KOPII ZAPASOWEJ**	**HARMONOGRAM** **Schematy tworzenia kopii zapasowych** **(nie dotyczy chmury)**	**OKRES PRZECHOWYWANIA**
Dyski/woluminy (komputery fizyczne)	Wybór bezpośredni (s. 43) Reguły zasad (s. 43) Filtry plików (s. 60)	Chmura (s. 47) Folder lokalny (s. 47) Folder sieciowy (s. 47) NFS (s. 47)* Secure Zone (s. 47)**	Zawsze przyrostowa (jednoplikowa) (s. 50) Zawsze pełne (s. 50) Tygodniowe pełne, dzienne przyrostowe (s. 50) Niestandardowe (P-D-P) (s. 50)	Według wieku kopii zapasowych (jedna reguła na zestaw kopii zapasowych) (s. 51) Według liczby kopii zapasowych (s. 51) Zachowaj w nieskończoność (s. 51)
Dyski/woluminy (maszyny wirtualne)	Reguły zasad (s. 43) Filtry plików (s. 60)	Chmura (s. 47) Folder lokalny (s. 47) Folder sieciowy (s. 47) NFS (s. 47)*		
Pliki (tylko komputery fizyczne)	Wybór bezpośredni (s. 44) Reguły zasad (s. 44) Filtry plików (s. 60)	Chmura (s. 47) Folder lokalny (s. 47) Folder sieciowy (s. 47) NFS (s. 47)* Secure Zone (s. 47)**	Zawsze pełne (s. 50) Tygodniowe pełne, dzienne przyrostowe (s. 50) Niestandardowe (P-D-P) (s. 50)	

Copyright © Acronis International GmbH, 2002-2017

Konfiguracja ESXi	Wybór bezpośredni (s. 46)	Folder lokalny (s. 47) Folder sieciowy (s. 47) NFS (s. 47)*		
Stan systemu	Wybór bezpośredni (s. 46)	Chmura (s. 47) Folder lokalny (s. 47) Folder sieciowy (s. 47)	Zawsze pełne (s. 50) Tygodniowe pełne, dzienne przyrostowe (s. 50) Niestandardowe (P-P) (s. 50)	
Bazy danych SQL	Wybór bezpośredni (s. 110)			
Bazy danych programu Exchange	Wybór bezpośredni (s. 111)			
Skrzynki pocztowe Office 365	Wybór bezpośredni (s. 122)		Zawsze przyrostowa (jednoplikowa) (s. 50)	Według liczby kopii zapasowych (s. 51) Zachowaj w nieskończoność (s. 51)

* W systemie Windows tworzenie kopii zapasowych w udziałach NFS jest niedostępne.

** Na komputerze z systemem Mac nie można utworzyć strefy Secure Zone.

5.2 Wybieranie danych do uwzględnienia w kopii zapasowej

5.2.1 Wybieranie dysków/woluminów

Kopia zapasowa na poziomie dysku zawiera kopię dysku lub woluminu w postaci spakowanej. Z kopii zapasowej na poziomie dysku można odzyskiwać poszczególne dyski, woluminy lub pliki. W kopii zapasowej całego komputera są uwzględniane wszystkie jego dyski.

Dyski/woluminy można wybierać na dwa sposoby: bezpośrednio na każdym komputerze lub przy użyciu reguł zasad. Istnieje możliwość wykluczenia plików z kopii zapasowej dysku dzięki ustawieniu filtrów plików (s. 60).

Wybór bezpośredni

Wybór bezpośredni jest dostępny tylko w przypadku komputerów fizycznych.

1. W polu **Elementy uwzględniane w kopii zapasowej** wybierz **Dyski/woluminy**.
2. Kliknij **Elementy uwzględniane w kopii zapasowej**.
3. W polu **Wybierz elementy do uwzględnienia w kopii zapasowej** wybierz **Bezpośrednio**.
4. W przypadku każdego komputera objętego planem tworzenia kopii zapasowych zaznacz pola wyboru obok dysków lub woluminów, które mają być uwzględniane w kopii zapasowej.
5. Kliknij **Gotowe**.

Użycie reguł zasad

1. W polu **Elementy uwzględniane w kopii zapasowej** wybierz **Dyski/woluminy**.
2. Kliknij **Elementy uwzględniane w kopii zapasowej**.
3. W polu **Wybierz elementy do uwzględnienia w kopii zapasowej** wybierz **Użycie reguł zasad**.
4. Wybierz dowolne z gotowych reguł, wpisz własne reguły lub skorzystaj z obu tych możliwości.

   Reguły zasad będą stosowane do wszystkich komputerów objętych planem tworzenia kopii zapasowych. Jeśli w chwili rozpoczęcia tworzenia kopii zapasowej na komputerze nie zostaną

Copyright © Acronis International GmbH, 2002-2017

znalezione żadne dane spełniające wymagania co najmniej jednej reguły, utworzenie kopii zapasowej na tym komputerze nie powiedzie się.

5. Kliknij **Gotowe**.

Reguły dotyczące systemów Windows, Linux i OS X

- **`[All volumes]`** powoduje wybranie wszystkich woluminów na komputerach z systemem Windows i wszystkich zamontowanych woluminów na komputerach z systemem Linux lub OS X.

Reguły dotyczące systemu Windows

- Litera dysku (na przykład **C:**) powoduje wybranie woluminu z określoną literą dysku.
- **`[Fixed Volumes (Physical machines)]`** powoduje wybranie wszystkich woluminów komputerów fizycznych, z wyjątkiem nośników wymiennych. Woluminy stałe obejmują woluminy na urządzeniach SCSI, ATAPI, ATA, SSA, SAS i SATA oraz macierzy RAID.
- **`[BOOT+SYSTEM]`** powoduje wybranie woluminów systemowych i startowych. Ta kombinacja to minimalny zestaw danych, który umożliwia odzyskanie systemu operacyjnego z kopii zapasowej.
- **`[Disk 1]`** powoduje wybranie pierwszego dysku komputera i obejmuje wszystkie woluminy na tym dysku. Aby wybrać inny dysk, wpisz odpowiedni numer.

Reguły dotyczące systemu Linux

- **`/dev/hda1`** powoduje wybranie pierwszego woluminu pierwszego dysku twardego IDE.
- **`/dev/sda1`** powoduje wybranie pierwszego woluminu pierwszego dysku twardego SCSI.
- **`/dev/md1`** powoduje wybranie pierwszego dysku twardego programowej macierzy RAID.

Aby wybrać inne woluminy standardowe, określ **`/dev/xdyN`**, gdzie:

- „x” odpowiada typowi dysku
- „y” odpowiada numerowi dysku (a w przypadku pierwszego dysku, b w przypadku drugiego dysku itd.)
- „N” oznacza numer woluminu

Aby wybrać wolumin logiczny, określ jego nazwę wraz z nazwą grupy woluminów. Aby na przykład utworzyć kopie zapasowe dwóch woluminów logicznych: **lv_root** i **lv_bin**, które oba należą do grupy woluminów **vg_mymachine**, określ:

```
/dev/vg_mymachine/lv_root
/dev/vg_mymachine/lv_bin
```

Reguły dotyczące systemu OS X

- **`[Disk 1]`** powoduje wybranie pierwszego dysku komputera i obejmuje wszystkie woluminy na tym dysku. Aby wybrać inny dysk, wpisz odpowiedni numer.

5.2.2 Wybieranie plików/folderów

Kopia zapasowa na poziomie plików jest dostępna tylko w przypadku komputerów fizycznych.

Kopia zapasowa na poziomie plików nie wystarcza do odzyskania systemu operacyjnego. Wybierz opcję tworzenia kopii zapasowej plików, jeśli planujesz chronić tylko określone dane (na przykład bieżący projekt). Rozmiar kopii zapasowej będzie mniejszy, dzięki czemu w pamięci masowej zostanie więcej miejsca.

Pliki można wybierać na dwa sposoby: bezpośrednio na każdym komputerze lub przy użyciu reguł zasad. Obie te metody umożliwiają dodatkowe sprecyzowanie wyboru dzięki ustawieniu filtrów plików (s. 60).

Copyright © Acronis International GmbH, 2002-2017

Wybór bezpośredni

1. W polu **Elementy uwzględniane w kopii zapasowej** wybierz **Pliki/foldery**.
2. Kliknij **Elementy uwzględniane w kopii zapasowej**.
3. W polu **Wybierz elementy do uwzględnienia w kopii zapasowej** wybierz **Bezpośrednio**.
4. W przypadku każdego komputera objętego planem tworzenia kopii zapasowych:
   a. Kliknij **Wybierz pliki i foldery**.
   b. Kliknij **Folder lokalny** lub **Folder sieciowy**.

      Udział musi być dostępny z wybranego komputera.
   c. Przejdź do wymaganych plików/folderów lub wprowadź ścieżkę i kliknij przycisk strzałki. Jeśli zostanie wyświetlony monit, określ nazwę użytkownika i hasło w celu uzyskania dostępu do folderu udostępnionego.
   d. Wybierz wymagane pliki/foldery.
   e. Kliknij **Gotowe**.

Użycie reguł zasad

1. W polu **Elementy uwzględniane w kopii zapasowej** wybierz **Pliki/foldery**.
2. Kliknij **Elementy uwzględniane w kopii zapasowej**.
3. W polu **Wybierz elementy do uwzględnienia w kopii zapasowej** wybierz **Użycie reguł zasad**.
4. Wybierz dowolne z gotowych reguł, wpisz własne reguły lub skorzystaj z obu tych możliwości.

   Reguły zasad będą stosowane do wszystkich komputerów objętych planem tworzenia kopii zapasowych. Jeśli w chwili rozpoczęcia tworzenia kopii zapasowej na komputerze nie zostaną znalezione żadne dane spełniające wymagania co najmniej jednej reguły, utworzenie kopii zapasowej na tym komputerze się nie powiedzie.
5. Kliknij **Gotowe**.

Reguły wyboru dotyczące systemu Windows

- Pełna ścieżka pliku lub folderu, na przykład **D:\Praca\Tekst.doc** lub **C:\Windows**.
- Szablony:
  - **`[All Files]`** powoduje wybranie wszystkich plików na wszystkich woluminach komputera.
  - **`[All Profiles Folder]`** powoduje wybranie folderu, w którym znajdują się wszystkie profile użytkowników (zwykle **C:\Users** lub **C:\Documents and Settings**).
- Zmienne środowiskowe:
  - **`%ALLUSERSPROFILE%`** powoduje wybranie folderu, w którym znajdują się wspólne dane wszystkich profili użytkowników (zwykle **C:\ProgramData** lub **C:\Documents and Settings\All Users**).
  - **`%PROGRAMFILES%`** powoduje wybranie folderu Program Files (na przykład **C:\Program Files**).
  - **`%WINDIR%`** powoduje wybranie folderu, w którym znajdują się pliki systemu Windows (na przykład **C:\Windows**).

  Można korzystać z innych zmiennych środowiskowych lub łączyć zmienne środowiskowe i tekst. Na przykład w celu wybrania folderu Java w folderze Program Files wpisz: **%PROGRAMFILES%\Java**.

Reguły wyboru dotyczące systemu Linux

- Pełna ścieżka pliku lub katalogu. Na przykład w celu utworzenia kopii zapasowej pliku **plik.txt** znajdującego się na woluminie **/dev/hda3** zamontowanym w lokalizacji **/home/usr/docs**, określ ścieżkę **/dev/hda3/plik.txt** lub **/home/usr/docs/plik.txt**.

Copyright © Acronis International GmbH, 2002-2017

- **`/home`** powoduje wybranie katalogu głównego zwykłych użytkowników.
- **`/root`** powoduje wybranie katalogu głównego użytkownika root.
- **`/usr`** powoduje wybranie katalogu wszystkich programów użytkowników.
- **`/etc`** powoduje wybranie katalogu plików konfiguracyjnych systemu.

- Szablony:
  - **`[All Profiles Folder]`** powoduje wybranie folderu **/home**. Jest to folder, w którym domyślnie znajdują się wszystkie profile użytkowników.

Reguły wyboru dotyczące systemu OS X

- Pełna ścieżka pliku lub katalogu.
- Szablony:
  - **`[All Profiles Folder]`** powoduje wybranie folderu **/Users**. Jest to folder, w którym domyślnie znajdują się wszystkie profile użytkowników.

Przykłady:

- Aby uwzględnić w kopii zapasowej plik **plik.txt** znajdujący się na pulpicie, określ **/Users/<nazwa użytkownika>/Desktop/plik.txt**, gdzie <nazwa użytkownika> oznacza Twoją nazwę użytkownika.
- Aby uwzględnić w kopii zapasowej katalogi główne wszystkich użytkowników, określ **/Users**.
- Aby uwzględnić w kopii zapasowej katalog, w którym są zainstalowane aplikacje, określ **/Applications**.

5.2.3 Wybieranie stanu systemu

Kopia zapasowa stanu system jest dostępna tylko w przypadku komputerów z systemem Windows Vista lub nowszym.

Aby utworzyć kopię zapasową stanu systemu, w polu **Elementy uwzględniane w kopii zapasowej** wybierz **Stan systemu**.

Kopia zapasowa stanu systemu zawiera następujące pliki:

- Konfiguracja Harmonogramu zadań
- Magazyn metadanych usługi VSS
- Informacje konfiguracyjne licznika wydajności
- Usługa MSSearch
- Usługa inteligentnego transferu w tle
- Rejestr
- Instrumentacja zarządzania Windows
- Baza danych rejestracji klas usług składowych

5.2.4 Wybieranie konfiguracji ESXi

Kopia zapasowa konfiguracji hosta ESXi umożliwia odzyskanie hosta ESXi na komputer bez systemu operacyjnego. Operacja odzyskiwania jest realizowana z poziomu nośnika startowego.

Maszyny wirtualne działające na hoście nie są uwzględniane w kopii zapasowej. Można jednak osobno tworzyć ich kopie zapasowe i osobno je odzyskiwać.

Kopia zapasowa konfiguracji hosta ESXi obejmuje:

- Program ładujący oraz partycje banku startowego hosta

Copyright © Acronis International GmbH, 2002-2017

- Stan hosta (konfigurację sieci wirtualnej i pamięci masowej, klucze SSL, ustawienia sieci serwera oraz informacje o użytkownikach lokalnych)
- Rozszerzenia i poprawki zainstalowane lub przygotowane na hoście
- Plik dzienników

Wymagania wstępne

- W polu **Profil zabezpieczeń** konfiguracji hosta ESXi musi być włączony protokół SSH.
- Trzeba znać hasło do konta „root” na hoście ESXi.

Aby wybrać konfigurację ESXi

1. Przejdź do sekcji **VMware** > **Hosty i klastry**.
2. Przejdź do hostów ESXi, które chcesz uwzględnić w kopii zapasowej.
3. Wybierz hosty ESXi i kliknij **Kopia zapasowa**.
4. W polu **Elementy uwzględniane w kopii zapasowej** zaznacz **Konfiguracja ESXi**.
5. W polu **Hasło do konta „root” ESXi** określ hasło do konta „root” na każdym z wybranych hostów lub zastosuj jedno hasło do wszystkich hostów.

5.3 Wybieranie miejsca docelowego

Kliknij **Miejsce docelowe kopii zapasowej** i wybierz jedną z następujących opcji:

- **Chmura**

  Kopie zapasowe będą przechowywane w chmurowym centrum danych.

- **Foldery lokalne**

  W przypadku wybrania jednego komputera przejdź do folderu na tym komputerze lub wpisz ścieżkę folderu.

  W przypadku wybrania wielu komputerów wpisz ścieżkę folderu. Kopie zapasowe będą przechowywane w tym folderze na każdym wybranym komputerze fizycznym lub na komputerze, na którym jest zainstalowany agent dla maszyn wirtualnych. Jeśli ten folder nie istnieje, zostanie utworzony.

- **Folder sieciowy**

  Jest to folder udostępniony za pośrednictwem udziału sieciowego SMB/CIFS/DFS.

  Przejdź do wymaganego folderu udostępnionego lub wprowadź ścieżkę w następującym formacie:

  - W przypadku udziałów SMB/CIFS: `\\<nazwa hosta>\<ścieżka>\` lub `smb://<nazwa hosta>/<ścieżka>/`
  - W przypadku udziałów DFS: `\\<pełna nazwa domeny DNS>\<folder root DFS>\<ścieżka>`

    Na przykład: `\\przyklad.company.com\shared\files`

  Następnie kliknij przycisk strzałki. Jeśli zostanie wyświetlony monit, określ nazwę użytkownika i hasło w celu uzyskania dostępu do folderu udostępnionego.

- **Folder NFS** (dostępny na komputerach z systemem Linux lub OS X)

  Przejdź do wymaganego folderu NFS lub wprowadź ścieżkę w następującym formacie:

  `nfs://<nazwa hosta>/<wyeksportowany folder>:/<podfolder>`

  Następnie kliknij przycisk strzałki.

  W folderze NFS chronionym hasłem nie można utworzyć kopii zapasowej.

- Strefa **Secure Zone** (dostępna, jeśli taka strefa znajduje się na każdym wybranym komputerze)

Copyright © Acronis International GmbH, 2002-2017

Secure Zone to bezpieczna partycja na dysku komputera uwzględnianego w kopii zapasowej. Partycję tę trzeba utworzyć ręcznie przed skonfigurowaniem kopii zapasowej. Informacje na temat tworzenia strefy Secure Zone oraz jej zalet i wad można znaleźć w sekcji „Informacje o strefie Secure Zone” (s. 48).

5.3.1 Informacje o strefie Secure Zone

Secure Zone to bezpieczna partycja na dysku komputera uwzględnianego w kopii zapasowej. Można na niej przechowywać kopie zapasowe dysków lub plików danego komputera.

W przypadku fizycznej usterki dysku można stracić kopie zapasowe ze strefy Secure Zone. Dlatego strefa Secure Zone nie powinna być jedyną lokalizacją do przechowywania kopii zapasowych. W infrastrukturze przedsiębiorstwa strefa Secure Zone może służyć jako pośrednia lokalizacja kopii zapasowych, używana w przypadku, gdy standardowa lokalizacja jest tymczasowo niedostępna albo podłączona przez powolny lub obciążony kanał przesyłowy.

Dlaczego warto korzystać ze strefy Secure Zone?

Secure Zone:

- Umożliwia odzyskanie zawartości dysku na ten sam dysk, na którym znajduje się jego kopia zapasowa.
- Stanowi oszczędną i wygodną metodę ochrony danych przed usterkami oprogramowania, atakami wirusów i błędami użytkowników.
- Eliminuje konieczność użycia dodatkowego nośnika lub połączenia sieciowego w celu utworzenia kopii zapasowej bądź odzyskania danych. Szczególnie przydaje się to użytkownikom mobilnym.
- Może służyć jako podstawowe miejsce docelowe w przypadku korzystania z replikacji kopii zapasowych.

Ograniczenia

- Na komputerze Mac nie można wydzielić strefy Secure Zone.
- Secure Zone jest partycją lokalizowaną na dysku standardowym. Nie można jej utworzyć na dysku dynamicznym ani utworzyć jako wolumin logiczny (zarządzany przy użyciu menedżera LVM).
- Strefa Secure Zone jest formatowana w systemie plików FAT32. Ponieważ w systemie FAT32 rozmiar plików jest ograniczony do 4 GB, większe kopie zapasowe są dzielone podczas zapisywania w strefie Secure Zone. Nie ma to wpływu na procedurę ani szybkość odzyskiwania.
- Strefa Secure Zone nie obsługuje kopii zapasowych w formacie jednoplikowym (s. 147). Jeśli strefa Secure Zone zostanie ustawiona jako lokalizacja docelowa w planie tworzenia kopii zapasowych ze schematem tworzenia kopii zapasowych **Zawsze przyrostowa (jednoplikowa)**, schemat ten zostanie zmieniony na **Tygodniowe pełne, dzienne przyrostowe**.

Jak utworzenie strefy Secure Zone wpływa na dysk

- Strefa Secure Zone zawsze jest tworzona na końcu dysku twardego.
- 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, oprogramowanie zajmuje wolne miejsce na wybranych woluminach, zmniejszając proporcjonalnie ich rozmiar.
- Na woluminie powinno jednak pozostać wolne miejsce, wymagane do prawidłowego działania systemu operacyjnego i aplikacji (na przykład do tworzenia plików tymczasowych).

Copyright © Acronis International GmbH, 2002-2017

Oprogramowanie nie zmniejszy rozmiaru woluminu, na którym ilość wolnego miejsca jest lub stałaby się mniejsza niż 25 procent rozmiaru woluminu. Proporcjonalne zmniejszanie rozmiaru woluminów będzie kontynuowane tylko wtedy, gdy wszystkie woluminy na dysku będą zawierać 25 procent lub mniej wolnego miejsca.

Jak widać powyżej, lepiej nie ustawiać maksymalnego możliwego rozmiaru strefy Secure Zone. W efekcie na żadnym woluminie nie pozostanie wolne miejsce, wskutek czego system operacyjny lub aplikacje mogą działać niestabilnie lub w ogóle się nie uruchamiać.

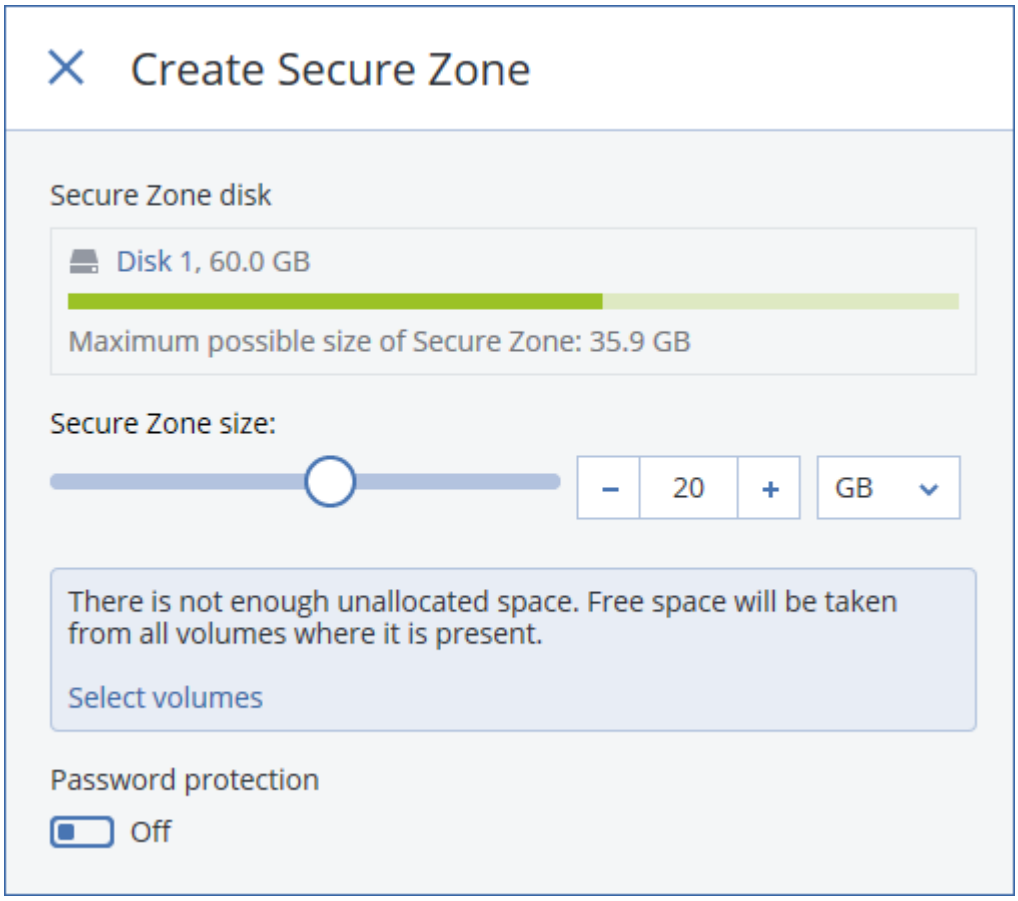
Ważne *Przeniesienie lub zmiana rozmiaru woluminu, z którego uruchamiany jest system, wymaga ponownego uruchomienia komputera.*

Jak utworzyć strefę Secure Zone

1. Wybierz komputer, na którym chcesz utworzyć strefę Secure Zone.
2. Kliknij **Przegląd** > **Utwórz strefę Secure Zone**.
3. W obszarze **Dysk strefy Secure Zone** kliknij **Wybierz**, a następnie wybierz dysk twardy (jeśli jest ich kilka), na którym ma zostać utworzona strefa.

   Oprogramowanie obliczy maksymalny rozmiar strefy Secure Zone.
4. Wprowadź rozmiar strefy Secure Zone lub przeciągnij suwak w celu wybrania dowolnego rozmiaru między wartościami minimalną i maksymalną.

   Minimalny rozmiar to 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 dysku.
5. Jeśli nieprzydzielonego miejsca jest zbyt mało na określony rozmiar, oprogramowanie zajmie wolne miejsce z istniejących woluminów. Domyślnie wybrane są wszystkie woluminy. Jeśli chcesz wykluczyć jakieś woluminy, kliknij **Wybierz woluminy**. W przeciwnym razie pomiń ten krok.



Copyright © Acronis International GmbH, 2002-2017

6. [Opcjonalnie] Włącz przełącznik **Ochrona hasłem** i określ hasło.

   Hasło to będzie wymagane podczas uzyskiwania dostępu do kopii zapasowych znajdujących się w strefie Secure Zone. Utworzenie kopii zapasowej w strefie Secure Zone nie wymaga hasła, chyba że kopia jest tworzona przy użyciu nośnika startego.
7. Kliknij **Utwórz**.

   Oprogramowanie wyświetli spodziewany układ partycji. Kliknij **OK**.
8. Poczekaj, aż oprogramowanie utworzy strefę Secure Zone.

Teraz podczas tworzenia planu tworzenia kopii zapasowych możesz w sekcji **Miejsce docelowe kopii zapasowej** wybrać strefę Secure Zone.

Jak usunąć strefę Secure Zone

1. Wybierz komputer ze strefą Secure Zone.
2. Kliknij **Przegląd**.
3. Kliknij ikonę koła zębatego widoczną obok strefy **Secure Zone**, a następnie kliknij **Usuń**.
4. [Opcjonalnie] Określ woluminy, do których zostanie dodane miejsce zwolnione przez strefę. Domyślnie wybrane są wszystkie woluminy.

   Miejsce zostanie równo rozdzielone między wybrane woluminy. W przypadku niewybrania żadnego woluminu zwolnione miejsce będzie nieprzydzielone.

   Zmiana rozmiaru woluminu, z którego uruchamiany jest system, wymaga ponownego uruchomienia komputera.
5. Kliknij **Usuń**.

W wyniku tego strefa Secure Zone zostanie usunięta wraz ze wszystkimi przechowywanymi w niej kopiami zapasowymi.

5.4 Harmonogram

Parametry harmonogramu zależą od docelowej lokalizacji kopii zapasowych.

W przypadku tworzenia kopii zapasowych w chmurze

Domyślnie kopie zapasowe są tworzone codziennie od poniedziałku do piątku. Można wybrać godzinę rozpoczęcia tworzenia kopii zapasowej.

Aby zmienić częstość tworzenia kopii zapasowych, przesuń suwak i określ harmonogram tworzenia kopii zapasowych.

Ważne *Pierwsza tworzona kopia zapasowa będzie pełna, a więc i najbardziej czasochłonna. Kolejne kopie zapasowe będą przyrostowe, więc ich utworzenie zajmie znacznie mniej czasu.*

W przypadku tworzenia kopii zapasowych w innych lokalizacjach

Można wybrać jeden z gotowych schematów tworzenia kopii zapasowych lub utworzyć schemat niestandardowy. Schemat tworzenia kopii zapasowych wchodzi w skład planu tworzenia kopii zapasowych, który obejmuje harmonogram oraz metody tworzenia kopii zapasowych.

W sekcji **Schemat tworzenia kopii zapasowych** wybierz jedno z następujących ustawień:

- [Tylko w przypadku kopii zapasowych na poziomie dysku] **Zawsze przyrostowa (jednoplikowa)**

  Domyślnie kopie zapasowe są tworzone codziennie od poniedziałku do piątku. Można wybrać godzinę rozpoczęcia tworzenia kopii zapasowej.

Copyright © Acronis International GmbH, 2002-2017

Aby zmienić częstość tworzenia kopii zapasowych, przesuń suwak i określ harmonogram tworzenia kopii zapasowych.

W przypadku tych kopii zapasowych będzie stosowany nowy format jednoplikowych kopii zapasowych (s. 147).

Opcja niedostępna w przypadku tworzenia kopii zapasowej w strefie Secure Zone.

- **Zawsze pełne**

  Domyślnie kopie zapasowe są tworzone codziennie od poniedziałku do piątku. Można wybrać godzinę rozpoczęcia tworzenia kopii zapasowej.

  Aby zmienić częstość tworzenia kopii zapasowych, przesuń suwak i określ harmonogram tworzenia kopii zapasowych.

  Wszystkie kopie zapasowe są pełne.

- **Tygodniowe pełne, dzienne przyrostowe**

  Domyślnie kopie zapasowe są tworzone codziennie od poniedziałku do piątku. Można zmodyfikować dni tygodnia i godziny tworzenia kopii zapasowych.

  Pełna kopia zapasowa jest tworzona raz w tygodniu. Pozostałe kopie zapasowe są przyrostowe. Dzień tworzenia pełnej kopii zapasowej zależy od opcji **Tygodniowa kopia zapasowa** (kliknij ikonę koła zębatego, a następnie **Opcje tworzenia kopii zapasowych** > **Tygodniowa kopia zapasowa**).

- **Niestandardowe**

  Określ harmonogramy pełnych, różnicowych i przyrostowych kopii zapasowych.

  Różnicowa kopia zapasowa nie jest dostępna w przypadku tworzenia kopii zapasowych danych SQL, danych programu Exchange lub stanu systemu.

Dodatkowe opcje planowania

W przypadku każdego miejsca docelowego można wykonać następujące czynności:

- Określić zakres dat wyznaczający okres obowiązywania harmonogramu. Zaznacz pole wyboru **Uruchom plan w danym przedziale dat**, a następnie określ zakres dat.
- Wyłączyć harmonogram. W przypadku wyłączenia harmonogramu reguły przechowywania nie będą stosowane, chyba że tworzenie kopii zapasowej zostanie uruchomione ręcznie.
- Wprowadzać opóźnienie w stosunku do zaplanowanej godziny. Wartość opóźnienia jest w przypadku każdego komputera wybierana losowo i mieści się w zakresie od zera do określonej przez Ciebie wartości maksymalnej. Ustawienia tego warto użyć w przypadku tworzenia kopii zapasowych wielu komputerów w lokalizacji sieciowej — pozwoli ono uniknąć nadmiernego obciążenia sieci.

  Kliknij ikonę koła zębatego, a następnie **Opcje tworzenia kopii zapasowych** > **Harmonogram**. Wybierz **Rozłóż uruchamianie operacji tworzenia kopii zapasowych w przedziale czasu** i określ maksymalne opóźnienie. Wartość opóźnienia dla poszczególnych komputerów jest ustalana podczas stosowania planu tworzenia kopii zapasowych na tych komputerach. Pozostaje ona niezmienna do chwili ewentualnej edycji planu i zmiany maksymalnej wartości opóźnienia.

***Uwaga** W przypadku wdrożeń chmurowych ta opcja jest domyślnie włączona, przy czym maksymalne opóźnienie jest ustawione na 30 minut. W przypadku wdrożeń lokalnych wszystkie operacje tworzenia kopii zapasowych domyślnie rozpoczynają się zgodnie z harmonogramem.*

5.5 Reguły przechowywania

1. Kliknij **Okres przechowywania**.
2. W polu **Czyszczenie** wybierz jedną z następujących opcji:
   - **Według wieku kopii zapasowych** (domyślna)

Copyright © Acronis International GmbH, 2002-2017

Określ czas przechowywania kopii zapasowych utworzonych w ramach planu tworzenia kopii zapasowych. Domyślnie reguły przechowywania określa się dla każdego zestawu kopii zapasowych (s. 147) z osobna. Aby użyć jednej reguły w przypadku wszystkich kopii zapasowych, kliknij **Zmień na jedną regułę dla wszystkich zestawów kopii zapasowych**.

- **Według liczby kopii zapasowych**

  Określ maksymalną liczbę przechowywanych kopii zapasowych.

- **Przechowuj kopie zapasowe bezterminowo**

Uwaga *Kopii zapasowej przechowywanej w folderze lokalnym lub sieciowym nie można usunąć, jeśli są od niej zależne inne kopie zapasowe, które nie kwalifikują się do usunięcia. Takie ciągi kopii zapasowych są usuwane dopiero wtedy, gdy upłynie czas przechowywania wszystkich ich kopii zapasowych. Wymagane jest więc dodatkowe miejsce na przechowywanie kopii zapasowych, których usunięcie zostało opóźnione. Ponadto wiek oraz liczba kopii zapasowych może przekraczać określone przez użytkownika wartości.*

5.6 Replikacja

W przypadku włączenia replikacji kopii zapasowych każda kopia zapasowa natychmiast po utworzeniu zostanie skopiowana do innej lokalizacji. Jeśli wcześniejsze kopie zapasowe nie zostały zreplikowane (na przykład z powodu utraty połączenia sieciowego), oprogramowanie zreplikuje również wszystkie kopie zapasowe, której pojawiły się po ostatniej pomyślnej replikacji.

Zreplikowane kopie zapasowe są niezależne od kopii zapasowych pozostałych w pierwotnej lokalizacji — i na odwrót. Dane można odzyskać z dowolnej kopii zapasowej bez dostępu do pozostałych lokalizacji.

Przykłady użycia

- **Niezawodne odzyskiwanie po awarii**

  Kopie zapasowe przechowuj zarówno lokalnie (w celu natychmiastowego odzyskania danych), jak i w innej lokalizacji (w celu zabezpieczenia kopii zapasowych przez awarią lokalnego magazynu lub klęską żywiołową).

- **Korzystanie z chmury w celu ochrony danych przed skutkami klęsk żywiołowych**

  Istnieje możliwość replikowania kopii zapasowych do chmury przez przesyłanie jedynie zmienionych danych.

- **Przechowywanie jedynie ostatnich punktów odzyskiwania**

  Usuwaj starsze kopie zapasowe z magazynu o szybkim dostępie zgodnie z regułami przechowywania, zapobiegając nadużywaniu kosztownego miejsca w pamięci masowej.

Obsługiwane lokalizacje

Kopię zapasową można zreplikować *z* dowolnej spośród następujących lokalizacji:

- Folder lokalny
- Folder sieciowy
- Secure Zone

Kopię zapasową można zreplikować *do* dowolnej spośród następujących lokalizacji:

- Folder lokalny
- Folder sieciowy
- Chmura

Aby włączyć replikację kopii zapasowych

1. W panelu planu tworzenia kopii zapasowych włącz przełącznik **Replikuj kopie zapasowe**.

Copyright © Acronis International GmbH, 2002-2017

Ten przełącznik jest widoczny tylko wtedy, gdy jest obsługiwana replikacja z lokalizacji wybranej w sekcji **Miejsce docelowe kopii zapasowej**.

2. W polu **Miejsce replikacji** określ miejsce docelowe replikacji zgodnie z instrukcjami podanymi w sekcji „Wybieranie miejsca docelowego” (s. 47).
3. W polu **Okres przechowywania** określ reguły przechowywania zgodnie z instrukcjami podanymi w sekcji „Reguły przechowywania” (s. 51).

5.7 Szyfrowanie

Zalecamy szyfrowanie wszystkich kopii zapasowych przechowywanych w chmurze, zwłaszcza jeśli firma podlega obowiązkowi zachowania zgodności ze stosownymi przepisami.

Ważne *W przypadku zgubienia lub zapomnienia hasła zaszyfrowanych kopii zapasowych nie da się odzyskać.*

Szyfrowanie w planie tworzenia kopii zapasowych

Aby włączyć szyfrowanie, określ ustawienia szyfrowania podczas tworzenia planu tworzenia kopii zapasowych. Po zastosowaniu planu tworzenia kopii zapasowych już nie będzie można zmienić ustawień szyfrowania. Jeśli chcesz użyć innych ustawień szyfrowania, utwórz nowy plan tworzenia kopii zapasowych.

Aby określić ustawienia szyfrowania w planie tworzenia kopii zapasowych

1. W panelu planu tworzenia kopii zapasowych włącz przełącznik **Szyfrowanie**.
2. Określ i potwierdź hasło szyfrowania.
3. Wybierz jeden z następujących algorytmów szyfrowania:
   - **AES 128** — kopie zapasowe będą szyfrowane przy użyciu algorytmu Advanced Encryption Standard (AES) z kluczem 128-bitowym.
   - **AES 192** — kopie zapasowe będą szyfrowane przy użyciu algorytmu AES z kluczem 192-bitowym.
   - **AES 256** — kopie zapasowe będą szyfrowane przy użyciu algorytmu AES z kluczem 256-bitowym.
4. Kliknij **OK**.

Szyfrowanie jako właściwość komputera

Ta opcja jest przeznaczona dla administratorów obsługujących kopie zapasowe wielu komputerów. Jeśli potrzebne jest unikatowe hasło dla każdego komputera lub trzeba wymusić szyfrowanie kopii zapasowych niezależnie od ustawień szyfrowania planu tworzenia kopii zapasowych, należy zapisać ustawienia szyfrowania na każdym komputerze z osobna.

Zapisanie ustawień szyfrowania na komputerze wpływa na plany tworzenia kopii zapasowych w sposób następujący:

- **Plany tworzenia kopii zapasowych już zastosowane do komputera.** Jeśli ustawienia szyfrowania w planie tworzenia kopii zapasowych są inne, nie uda się utworzyć kopii zapasowych.
- **Plany tworzenia kopii zapasowych, które zostaną zastosowane do komputera później.** Ustawienia szyfrowania zapisane na komputerze zastąpią ustawienia szyfrowania w planie tworzenia kopii zapasowych. Wszystkie kopie zapasowe zostaną zaszyfrowane, nawet jeśli szyfrowanie jest wyłączone w ustawieniach planu tworzenia kopii zapasowych.

Po zapisaniu ustawień nie będzie można ich zmienić, ale będzie można je zresetować zgodnie z poniższymi instrukcjami.

Copyright © Acronis International GmbH, 2002-2017

Ta opcja jest dostępna w przypadku komputerów z systemem Windows lub Linux. Nie jest obsługiwana w systemie OS X.

Tej opcji można użyć na komputerze z uruchomionym agentem dla VMware. Jeśli jednak do danego serwera vCenter jest podłączony więcej niż jeden agent dla VMware, należy zachować ostrożność. W przypadku każdego z tych agentów trzeba użyć tych samych ustawień szyfrowania, ponieważ występuje między nimi pewnego rodzaju równoważenie obciążenia.

Aby zapisać ustawienia szyfrowania na komputerze

1. Zaloguj się jako administrator (w systemie Windows) lub użytkownik root (w systemie Linux).
2. Uruchom następujący skrypt:
   - W systemie Windows: `<ścieżka_instalacji>`**\PyShell\bin\acropsh.exe -m manage_creds --set-password** `<hasło_szyfrowania>`

     Zmienna `<ścieżka_instalacji>` oznacza ścieżkę instalacji agenta kopii zapasowych. W przypadku wdrożeń chmurowych domyślnie jest to ścieżka **%ProgramFiles%\BackupClient**, a w przypadku wdrożeń lokalnych ścieżka **%ProgramFiles%\Acronis**.
   - W systemie Linux: **/usr/sbin/acropsh -m manage_creds --set-password** `<hasło_szyfrowania>`

Kopie zapasowe zostaną zaszyfrowane przy użyciu algorytmu AES z kluczem 256-bitowym.

Aby zresetować ustawienia szyfrowania na komputerze

1. Zaloguj się jako administrator (w systemie Windows) lub użytkownik root (w systemie Linux).
2. Uruchom następujący skrypt:
   - W systemie Windows: `<ścieżka_instalacji>`**\PyShell\bin\acropsh.exe -m manage_creds --reset**

     Zmienna `<ścieżka_instalacji>` oznacza ścieżkę instalacji agenta kopii zapasowych. W przypadku wdrożeń chmurowych domyślnie jest to ścieżka **%ProgramFiles%\BackupClient**, a w przypadku wdrożeń lokalnych ścieżka **%ProgramFiles%\Acronis**.
   - W systemie Linux: **/usr/sbin/acropsh -m manage_creds --reset**

Ważne *Po zresetowaniu ustawień szyfrowania na komputerze tworzenie kopii zapasowych tego komputera będzie się kończyć niepowodzeniem. Aby nadal tworzyć kopie zapasowe tego komputera, należy utworzyć nowy plan tworzenia kopii zapasowych.*

Jak działa szyfrowanie

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 kopii zapasowych, ale dane są 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 ani w kopiach zapasowych — do celów weryfikacji służy skrót hasła. Dzięki tym dwupoziomowym zabezpieczeniom dane kopii zapasowej są chronione przed nieautoryzowanym dostępem, ale odzyskanie utraconego hasła jest niemożliwe.

5.8 Ręczne rozpoczynanie tworzenia kopii zapasowych

1. Wybierz komputer z co najmniej jednym planem tworzenia kopii zapasowych.
2. Kliknij **Kopia zapasowa**.

Copyright © Acronis International GmbH, 2002-2017

3. Jeśli jest stosowany więcej niż jeden plan tworzenia kopii zapasowych, wybierz odpowiedni plan.
4. Kliknij **Uruchom teraz** w panelu planu tworzenia kopii zapasowych.

Postęp operacji tworzenia kopii zapasowej jest widoczny w kolumnie **Status** komputera.

5.9 Opcje tworzenia kopii zapasowych

Aby zmodyfikować opcje tworzenia kopii zapasowych, kliknij ikonę koła zębatego widoczną obok nazwy planu tworzenia kopii zapasowych, a następnie kliknij **Opcje tworzenia kopii zapasowych**.

Dostępne opcje tworzenia kopii zapasowych

Zakres dostępnych opcji tworzenia kopii zapasowych zależy od następujących czynników:

- Środowisko działania agenta (Windows, Linux, OS X)
- Typ danych uwzględnianych w kopii zapasowej (dyski, pliki, maszyny wirtualne, dane aplikacji)
- Lokalizacja docelowa kopii zapasowej (chmura, folder lokalny lub sieciowy).

W poniższej tabeli zestawiono dostępność opcji tworzenia kopii zapasowych.

	Tworzenie kopii zapasowych na poziomie dysku			**Kopia zapasowa na poziomie plików**			**Maszyny wirtualne**		**SQL oraz Exchange**
	Windows	Linux	OS X	Windows	Linux	OS X	ESXi	Hyper-V	Windows
Konsolidacja kopii zapasowych (s. 57)	+	+	+	+	+	+	+	+	-
Sprawdzanie poprawności kopii zapasowej (s. 57)	+	+	+	+	+	+	+	+	+
CBT (Changed Block Tracking) (s. 58)	+	-	-	-	-	-	+	+	-
Stopień kompresji (s. 58)	+	+	+	+	+	+	+	+	+
Powiadomienia e-mail (s. 58)	+	+	+	+	+	+	+	+	+
Obsługa błędów (s. 59)									
W razie błędu spróbuj ponownie	+	+	+	+	+	+	+	+	+
Nie pokazuj komunikatów ani okien dialogowych podczas przetwarzania (tryb dyskretny)	+	+	+	+	+	+	+	+	+
Ignoruj uszkodzone sektory	+	+	+	+	+	+	+	+	-
W razie błędu tworzenia migawki maszyny wirtualnej spróbuj ponownie	-	-	-	-	-	-	+	+	-
Szybka przyrostowa/różnicowa kopia zapasowa (s. 60)	+	+	+	-	-	-	-	-	-

Copyright © Acronis International GmbH, 2002-2017

	Tworzenie kopii zapasowych na poziomie dysku			Kopia zapasowa na poziomie plików			Maszyny wirtualne		SQL oraz Exchange
	Windows	Linux	OS X	Windows	Linux	OS X	ESXi	Hyper-V	Windows
Migawka kopii zapasowej na poziomie plików (s. 61)	-	-	-	+	+	+	-	-	-
Zabezpieczenia na poziomie plików (s. 62)	-	-	-	+	-	-	-	-	-
Filtry plików (s. 60)	+	+	+	+	+	+	+	+	-
Obcinanie dziennika (s. 62)	-	-	-	-	-	-	+	+	Tylko SQL
Wykonywanie migawek LVM (s. 63)	-	+	-	-	-	-	-	-	-
Punkty zamontowania (s. 63)	-	-	-	+	-	-	-	-	-
Migawka wielowoluminowa (s. 64)	+	-	-	+	-	-	-	-	-
Wydajność (s. 64)	+	+	+	+	+	+	+	+	+
Polecenia poprzedzające/następujące (s. 65)	+	+	+	+	+	+	+	+	+
Polecenia poprzedzające rejestrowanie danych/następujące po nim (s. 67)	+	+	+	+	+	+	-	-	+
Tworzenie harmonogramu (s. 69)									
Rozłóż uruchamianie w przedziale czasu	+	+	+	+	+	+	+	+	+
Ogranicz liczbę jednoczesnych operacji tworzenia kopii zapasowych	-	-	-	-	-	-	+	+	-
Kopia zapasowa sektor po sektorze (s. 70)	+	+	-	-	-	-	+	+	-
Dzielenie (s. 70)	+	+	+	+	+	+	+	+	+
Obsługa niepowodzenia zadania (s. 70)	+	+	+	+	+	+	+	+	+
Usługa kopiowania woluminów w tle (VSS) (s. 70)	+	-	-	+	-	-	-	+	+
Usługa kopiowania woluminów w tle (VSS) dla maszyn wirtualnych (s. 72)	-	-	-	-	-	-	+	+	-
Tygodniowa kopia zapasowa (s. 72)	+	+	+	+	+	+	+	+	+

Copyright © Acronis International GmbH, 2002-2017

	Tworzenie kopii zapasowych na poziomie dysku			Kopia zapasowa na poziomie plików			Maszyny wirtualne		SQL oraz Exchange
	Windows	Linux	OS X	Windows	Linux	OS X	ESXi	Hyper-V	Windows
Dziennik zdarzeń systemu Windows (s. 72)	+	-	-	+	-	-	+	+	+

5.9.1 Konsolidacja kopii zapasowych

Ta opcja jest dostępna w przypadku schematów tworzenia kopii zapasowych **Zawsze pełne**; **Tygodniowe pełne, dzienne przyrostowe** oraz **Niestandardowy**.

Ustawienie wstępne: **Wyłączone**.

Konsolidacja to proces polegający na połączeniu co najmniej dwóch kolejnych kopii zapasowych w jedną.

W przypadku włączenia tej opcji kopia zapasowa, która powinna zostać usunięta podczas czyszczenia, zostanie skonsolidowana z następną zależną kopią zapasową (przyrostową lub różnicową).

Jeśli opcja nie zostanie włączona, kopia zapasowa zostanie zachowana do czasu, gdy wszystkie zależne kopie zapasowe będą się kwalifikowały do usunięcia. Pomaga to uniknąć potencjalnie czasochłonnej konsolidacji, ale wymaga dodatkowego miejsca na przechowywanie kopii zapasowych, których usunięcie zostało opóźnione. Wiek bądź liczba kopii zapasowych może przekroczyć wartości określone w regułach przechowywania.

Ważne *Należy pamiętać, że konsolidacja to po prostu metoda usuwania, a nie alternatywa dla 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.*

5.9.2 Sprawdzanie poprawności kopii zapasowej

Operacja sprawdzania poprawności polega na sprawdzeniu, czy można odzyskać dane z kopii zapasowej. W przypadku włączenia tej opcji każda kopia zapasowa utworzona w ramach planu tworzenia kopii zapasowych jest od razu sprawdzana pod kątem poprawności.

Ustawienie wstępne: **Wyłączone**.

Operacja sprawdzania poprawności polega na obliczeniu sumy kontrolnej każdego bloku danych, który można odzyskać z danej kopii zapasowej. Jedynym wyjątkiem jest sprawdzanie poprawności kopii zapasowych na poziomie plików znajdujących się w chmurze. Sprawdzenie poprawności tych kopii zapasowych polega na sprawdzeniu spójności zapisanych w nich metadanych.

Sprawdzanie poprawności jest czasochłonne — nawet w przypadku przyrostowych lub różnicowych kopii zapasowych, które mają niewielkie rozmiary. Dzieje się tak, ponieważ w trakcie tej operacji sprawdzana jest poprawność nie tylko danych zawartych fizycznie w kopii zapasowej, ale również wszystkich danych, które można odzyskać po wybraniu tej kopii. Wymaga to uzyskania dostępu do utworzonych wcześniej kopii zapasowych.

Copyright © Acronis International GmbH, 2002-2017

Pomyślny wynik sprawdzania poprawności oznacza wysokie prawdopodobieństwo poprawnego odzyskania danych, ale kontrola taka nie obejmuje weryfikacji wszystkich czynników wpływających na proces odzyskiwania. W przypadku kopii zapasowej systemu operacyjnego zaleca się przeprowadzenie odzyskiwania testowego na zapasowy dysk twardy za pomocą nośnika startowego lub uruchomienie maszyny wirtualnej z kopii zapasowej (s. 123) w środowisku ESXi bądź Hyper-V.

5.9.3 CBT (Changed Block Tracking)

Ta opcja jest dostępna w przypadku kopii zapasowych na poziomie dysku uwzględniających maszyny wirtualne i/lub komputery fizyczne z systemem Windows.

Ustawienie wstępne: **Włączona**.

Ta opcja określa, czy podczas tworzenia przyrostowej lub różnicowej kopii zapasowej ma być używana funkcja Changed Block Tracking (CBT).

Technologia CBT przyspiesza proces tworzenia kopii zapasowych. Zmiany zawartości dysku są stale monitorowane na poziomie bloków. Po rozpoczęciu tworzenia kopii zapasowej zmiany mogą zostać niezwłocznie zapisane w kopii zapasowej.

5.9.4 Stopień kompresji

Ta opcja określa stopień kompresji danych w tworzonej kopii zapasowej. Dostępne są następujące poziomy: **Brak**, **Normalny**, **Wysoki**.

Ustawienie wstępne: **Normalny**.

Wyższy poziom kompresji powoduje, że utworzenie kopii zapasowej trwa dłużej, ale wynikowa kopia zapasowa zajmuje mniej miejsca.

Optymalny poziom kompresji danych zależy od typu danych uwzględnianych w kopii zapasowej. Nawet maksymalna kompresja nie wpłynie w sposób istotny na zmniejszenie rozmiaru kopii zapasowej, jeśli są w niej uwzględniane zasadniczo już skompresowane pliki, na przykład w formacie .jpg, .pdf lub .mp3. Jednak pliki w takich formatach jak .doc czy .xls zostaną dobrze skompresowane.

5.9.5 Powiadomienia e-mail

Ta opcja umożliwia skonfigurowanie powiadomień e-mail o błędach, ostrzeżeniach i pomyślnym wykonaniu kopii zapasowych.

Ta opcja jest dostępna wyłącznie w przypadku wdrożeń lokalnych. W przypadku wdrożeń chmurowych ustawienia są konfigurowane dla poszczególnych kont podczas ich tworzenia (s. 142).

Ustawienie wstępne: **Użyj ustawień domyślnych.**

Można użyć ustawień domyślnych lub zastąpić je wartościami niestandardowymi stosowanymi tylko w odniesieniu do tego planu. Ustawienia domyślne są konfigurowane zgodnie z opisem podanym w sekcji „Powiadomienia e-mail” (s. 140).

Ważne *Zmiana ustawień domyślnych wpłynie na wszystkie korzystające z nich plany tworzenia kopii zapasowych.*

Zanim włączysz tę opcję, upewnij się, że zostały skonfigurowane ustawienia **serwera poczty e-mail** (s. 139).

Copyright © Acronis International GmbH, 2002-2017

Aby dostosować powiadomienia e-mail dla planu tworzenia kopii zapasowych

1. Zaznacz **Dostosuj ustawienia na potrzeby tego planu tworzenia kopii zapasowych**.
2. W polu **Adresy e-mail odbiorców** wpisz docelowy adres e-mail. Możesz wprowadzić kilka adresów oddzielonych średnikami.
3. Wybierz typy powiadomień, które mają być wysyłane. Dostępne są następujące typy:
   - **Błędy**
   - **Ostrzeżenia**
   - **Udane kopie zapasowe**

Temat wiadomości e-mail ma następującą strukturę: **[temat] [nazwa komputera] [nazwa planu tworzenia kopii zapasowych]**. Zmienna **[temat]** jest zastępowana jednym z następujących tekstów: **Pomyślnie utworzono kopię zapasową**, **Utworzenie kopii zapasowej nie powiodło się**, **Kopia zapasowa została utworzona z ostrzeżeniami**.

5.9.6 Obsługa błędów

Umożliwiają one określenie sposobu obsługi błędów, które mogą wystąpić podczas tworzenia kopii zapasowej.

W razie błędu spróbuj ponownie

Ustawienie wstępne: **Włączone. Liczba prób: 30. Odstęp między próbami: 30 s.**

Po wystąpieniu błędu, który można naprawić, program próbuje ponownie wykonać operację zakończoną niepowodzeniem. Można ustawić odstęp między 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 sieciowa lokalizacja docelowa kopii zapasowej będzie niedostępna lub nieosiągalna, program będzie próbował nawiązać połączenie co 30 sekund, ale nie więcej niż 30 razy. Próby zostaną wstrzymane po wznowieniu połączenia LUB po wykonaniu określonej liczby prób, w zależności od tego, który warunek zostanie spełniony wcześniej.

***Uwaga** W przypadku wybrania chmury jako podstawowej lub drugiej lokalizacji docelowej opcja ta ma automatycznie ustawianą wartość **Włączono**. **Liczba prób: 300**.*

Nie pokazuj komunikatów ani okien dialogowych podczas przetwarzania (tryb dyskretny)

Ustawienie wstępne: **Włączona**.

Po włączeniu trybu dyskretnego program automatycznie obsługuje sytuacje wymagające działania użytkownika (poza obsługą uszkodzonych sektorów, 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.

Ignoruj uszkodzone sektory

Ustawienie wstępne: **Wyłączone**.

W przypadku wyłączenia tej opcji za każdym razem, gdy program napotka uszkodzony sektor, działaniu tworzenia kopii zapasowej zostanie przypisany status **Wymagane działanie**. Aby utworzyć kopię zapasową prawidłowych danych z dysku, któremu grozi nagła awaria, włącz ignorowanie

Copyright © Acronis International GmbH, 2002-2017

uszkodzonych sektorów. Pozostałe dane zostaną uwzględnione w kopii zapasowej, a po zamontowaniu wynikowej kopii zapasowej dysku będzie można wyodrębnić prawidłowe pliki na innym dysku.

W razie błędu tworzenia migawki maszyny wirtualnej spróbuj ponownie

Ustawienie wstępne: **Włączone. Liczba prób: 3. Odstęp między próbami: 5 minut.**

W razie niepowodzenia wykonania migawki maszyny wirtualnej program ponownie próbuje wykonać operację, która zakończyła się niepowodzeniem. Można ustawić odstęp między 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.

5.9.7 Szybka przyrostowa/różnicowa kopia zapasowa

Jest ona dostępna podczas tworzenia przyrostowych i różnicowych kopii zapasowych na poziomie dysku.

Ustawienie wstępne: **Włączona**.

W przyrostowej lub różnicowej kopii zapasowej są rejestrowane tylko zmiany danych. Aby przyspieszyć proces tworzenia kopii zapasowej, program ustala, czy plik się zmienił, na podstawie jego rozmiaru oraz daty/godziny jego ostatniej modyfikacji. Wyłączenie tej funkcji spowoduje, że program będzie porównywać całą zawartość plików z tymi przechowywanymi w kopii zapasowej.

5.9.8 Filtry plików

Filtry plików umożliwiają określenie, które pliki i foldery mają zostać pominięte w procesie tworzenia kopii zapasowej.

Jeśli nie zostanie określone inaczej, filtry plików są dostępne w przypadku tworzenia kopii zapasowych zarówno na poziomie dysku, jak i na poziomie plików.

Aby włączyć filtry plików

1. Wybierz dane do uwzględnienia w kopii zapasowej.
2. Kliknij ikonę koła zębatego widoczną obok nazwy planu tworzenia kopii zapasowych, a następnie kliknij **Opcje tworzenia kopii zapasowych**.
3. Wybierz **Filtry plików**.
4. Użyj dowolnych z niżej opisanych opcji.

Wyklucz pliki spełniające określone kryteria

Dostępne są dwie opcje o odwrotnym działaniu.

- **Uwzględnij w kopii zapasowej tylko pliki spełniające następujące kryteria**

  Przykład: Jeśli podczas tworzenia kopii zapasowej całego komputera w kryteriach filtrów zostanie określony plik **C:\Plik.exe**, w kopii zapasowej zostanie uwzględniony tylko ten plik.

  ***Uwaga** Ten filtr nie działa w przypadku kopii zapasowych na poziomie plików, chyba że lokalizacją docelową kopii zapasowej jest chmura.*

- **Nie uwzględniaj w kopii zapasowej plików spełniających następujące kryteria**

  Przykład: Jeśli podczas tworzenia kopii zapasowej całego komputera w kryteriach filtrów zostanie określony plik **C:\Plik.exe**, zostanie pominięty tylko ten plik.

Copyright © Acronis International GmbH, 2002-2017

Można używać obu opcji jednocześnie. Druga z wymienionych opcji ma pierwszeństwo, tj. w przypadku określenia pliku **C:\Plik.exe** w obu polach plik ten zostanie pominięty podczas tworzenia kopii zapasowej.

Kryteria

- **Pełna ścieżka**

  Określ pełną ścieżkę pliku lub folderu, zaczynając od litery dysku (w przypadku tworzenia kopii zapasowej danych w systemie Windows) lub katalogu głównego (w przypadku tworzenia kopii zapasowej danych w systemie Linux lub OS X).

  Zarówno w systemie Windows, jak i Linux / OS X w ścieżce pliku lub folderu można używać ukośnika (np. **C:/Temp/Plik.tmp**). W systemie Windows można też używać tradycyjnego ukośnika odwrotnego (np. **C:\Temp\Plik.tmp**).

- **Nazwa**

  Określ nazwę pliku lub folderu, na przykład **Dokument.txt**. Zostaną wybrane wszystkie pliki i foldery o tej nazwie.

W kryteriach *nie* jest uwzględniana wielkość liter. Na przykład w przypadku określenia ścieżki **C:\Temp** zostaną też wybrane ścieżki **C:\TEMP**, **C:\temp** itd.

W kryterium można używać symboli wieloznacznych (* i ?). Można ich używać zarówno w pełnej ścieżce, jak i w nazwie pliku lub folderu.

Gwiazdka (*) zastępuje zero lub więcej znaków w nazwie pliku. Na przykład kryterium **Dok*.txt** obejmuje zarówno plik **Dok.txt**, jak i **Dokument.txt**

Znak zapytania (?) zastępuje dokładnie jeden znak w nazwie pliku. Na przykład kryterium **Dok?.txt** obejmuje takie pliki jak **Dok1.txt** i **Doki.txt**, ale nie plik **Dok.txt** ani **Dok11.txt**.

Wyklucz pliki i foldery ukryte

Zaznacz to pole wyboru, aby pominąć pliki i foldery z atrybutem **Ukryty** (w przypadku systemów plików obsługiwanych w systemie Windows) lub o nazwie rozpoczynającej się od kropki (.) (w przypadku systemów plików w systemie Linux, takich jak Ext2 i Ext3). Jeśli folder jest ukryty, program wykluczy całą jego zawartość (w tym również pliki, które nie są ukryte).

Wyklucz pliki i foldery systemowe

Opcja ta ma zastosowanie tylko w przypadku systemów plików, które są obsługiwane przez system Windows. Zaznacz to pole wyboru, aby pominąć pliki i foldery z atrybutem **Systemowy**. Jeśli folder ma atrybut **Systemowy**, zostanie wykluczona cała jego zawartość (w tym pliki bez atrybutu **Systemowy**).

Wskazówka *Atrybuty pliku lub folderu można sprawdzić we właściwościach pliku lub folderu lub przy użyciu polecenia attrib. Więcej informacji można znaleźć w Centrum pomocy i obsługi technicznej w systemie Windows.*

5.9.9 Migawka kopii zapasowej na poziomie plików

Ta opcja jest dostępna tylko w przypadku kopii zapasowej na poziomie plików.

Ta opcja określa, czy kopia zapasowa ma być tworzona kolejno dla poszczególnych plików, czy też jako szybka migawka.

Uwaga *Pliki przechowywane w udziałach sieciowych zawsze są pojedynczo dodawane do kopii zapasowej.*

Copyright © Acronis International GmbH, 2002-2017

Ustawienie wstępne: **Utwórz migawkę, jeśli to możliwe**.

Możesz wybrać jedną z następujących opcji:

- **Utwórz migawkę, jeśli to możliwe**

  Jeśli nie można wykonać migawki, należy utworzyć bezpośrednią kopię zapasową plików.
- **Zawsze twórz migawkę**

  Migawka pozwala na utworzenie kopii zapasowej wszystkich plików, w tym plików, do których dostęp jest ograniczony. W kopii zapasowej zostaną uwzględnione pliki z tego samego punktu w czasie. Wybierz to ustawienie tylko wtedy, gdy są to krytyczne kwestie, tj. gdy nie ma sensu tworzyć kopii zapasowej plików bez migawki. Jeśli nie można utworzyć migawki, utworzenie kopii zapasowej zakończy się niepowodzeniem.
- **Nie twórz migawki**

  Zawsze wykonuj bezpośrednią kopię zapasową plików. Próba utworzenia kopii zapasowej plików otwartych do wyłącznego dostępu zakończy się błędem odczytu. Pliki w kopii zapasowej mogą być niespójne czasowo.

5.9.10 Zabezpieczenia na poziomie plików

Ta opcja jest dostępna tylko w przypadku kopii zapasowych na poziomie plików w systemie Windows.

Ta opcja określa, czy w kopii zapasowej plików należy również uwzględnić uprawnienia z systemu NTFS.

Ustawienie wstępne: **Włączone.**

W przypadku włączenia tej opcji pliki i foldery są uwzględniane w kopii zapasowej z oryginalnymi uprawnieniami do odczytu, zapisywania lub wykonywania plików dla każdego użytkownika lub grupy użytkowników. Odzyskanie zabezpieczonego pliku lub folderu na komputerze bez konta użytkownika określonego w uprawnieniach może skutkować brakiem możliwości odczytania lub modyfikacji tego pliku.

W przypadku wyłączenia tej opcji odzyskiwane pliki i foldery odziedziczą uprawnienia z folderu, do którego zostaną odzyskane, lub z dysku w przypadku odzyskania do katalogu głównego.

Można również wyłączyć odzyskiwanie (s. 88) ustawień zabezpieczeń. Efekt będzie taki sam: pliki odziedziczą uprawnienia z folderu nadrzędnego.

5.9.11 Obcinanie dziennika

Ta opcja jest dostępna w przypadku tworzenia kopii zapasowej baz danych programu Microsoft SQL Server oraz kopii zapasowej na poziomie dysku przy włączonym tworzeniu kopii zapasowej aplikacji Microsoft SQL Server.

Opcja umożliwia określenie, czy po pomyślnym utworzeniu kopii zapasowej mają być obcinane dzienniki transakcji programu SQL Server.

Ustawienie wstępne: **Włączona**.

W przypadku włączenia tej opcji bazę danych można odzyskać tylko do punktu w czasie kopii zapasowej utworzonej przez oprogramowanie. Tworząc kopię zapasową dzienników transakcji za pomocą macierzystego aparatu tworzenia kopii zapasowych programu Microsoft SQL Server, opcję tę należy wyłączyć. Po odzyskaniu można zastosować dzienniki transakcji i dzięki temu odzyskać bazę danych do dowolnego punktu w czasie.

Copyright © Acronis International GmbH, 2002-2017

5.9.12 Wykonywanie migawek LVM

Ta opcja jest dostępna tylko w przypadku komputerów fizycznych.

Opcja jest dostępna w przypadku tworzenia kopii zapasowej na poziomie dysku uwzględniającej woluminy zarządzane przez narzędzie Logical Volume Manager (LVM) systemu Linux. Woluminy takie określa się także mianem woluminów logicznych.

Ta opcja określa sposób wykonywania migawki woluminu logicznego. Program do tworzenia kopii zapasowych może wykonywać tę operację samodzielnie lub przy użyciu narzędzia Logical Volume Manager (LVM) systemu Linux.

Ustawienie wstępne: **Za pomocą oprogramowania do tworzenia kopii zapasowych**.

- **Za pomocą oprogramowania do tworzenia kopii zapasowych**. Dane migawki są przechowywane głównie w pamięci RAM. Dzięki temu kopie zapasowe są tworzone szybciej i nie jest potrzebne nieprzydzielone miejsce w grupie woluminów. Dlatego zaleca się zmianę ustawienia wstępnego tylko w przypadku problemów z tworzeniem kopii zapasowych woluminów logicznych.
- **Za pomocą menedżera LVM**. Migawka jest zapisywana w nieprzydzielonym miejscu w grupie woluminów. Jeśli nie ma nieprzydzielonego miejsca, migawka zostanie wykonana przez oprogramowanie do tworzenia kopii zapasowych.

5.9.13 Punkty zamontowania

Ta opcja jest dostępna tylko w systemie Windows do tworzenia kopii zapasowej na poziomie pliku źródła danych obejmującego zamontowane woluminy lub woluminy udostępnione w klastrze.

Ta opcja jest dostępna tylko w przypadku, gdy folder wybrany do utworzenia kopii zapasowej znajduje się wyżej w hierarchii folderów niż punkt zamontowania. (punkt zamontowania to folder, do którego został logicznie podłączony dodatkowy wolumin).

- Jeśli taki folder (folder nadrzędny) zostanie wybrany do utworzenia kopii zapasowej, a opcja **Punkty zamontowania** jest włączona, w kopii zapasowej będą uwzględnione wszystkie pliki znajdujące się w zamontowanym woluminie. Jeśli opcja **Punkty zamontowania** jest wyłączona, punkt zamontowania w kopii zapasowej będzie pusty.

  Odzyskanie zawartości punktu zamontowania podczas odzyskiwania folderu nadrzędnego zależy od wartości opcji odzyskiwania **Punkty zamontowania** (s. 89).
- Jeśli wybierzesz punkt zamontowania bezpośrednio lub wybierzesz dowolny folder na woluminie zamontowania, wybrane foldery będą traktowane jak foldery zwykłe. Zostaną uwzględnione w kopii zapasowej niezależnie od stanu opcji **Punkty zamontowania** i odzyskane bez względu na stan opcji odzyskiwania **Punkty zamontowania** (s. 89).

Ustawienie wstępne: **Wyłączone**.

Wskazówka. *Kopię zapasową maszyn wirtualnych Hyper-V znajdujących się w woluminie udostępnionym w klastrze tworzy się przez wykonanie kopii zapasowej na poziomie pliku wymaganych plików lub całego woluminu. Należy tylko pamiętać o wyłączeniu maszyn wirtualnych, aby ich kopia zapasowa była spójna.*

Przykład

Przyjmijmy, że folder **C:\Dane1** to punkt zamontowania zamontowanego woluminu. Wolumin zawiera foldery **Folder1** i **Folder2**. Tworzysz plan tworzenia kopii zapasowej danych na poziomie pliku.

Copyright © Acronis International GmbH, 2002-2017

Jeśli zaznaczysz pole wyboru woluminu C i włączysz opcję **Punkty zamontowania**, folder **C:\Dane1** w kopii zapasowej będzie zawierać foldery **Folder1** i **Folder2**. Podczas odzyskiwania danych z kopii zapasowej należy pamiętać o poprawnym zastosowaniu opcji odzyskiwania **Punkty zamontowania** (s. 89).

Jeśli zaznaczysz pole wyboru woluminu C i wyłączysz opcję **Punkty zamontowania**, folder **C:\Dane1** w kopii zapasowej będzie pusty.

Jeśli zaznaczysz pole wyboru folderu **Dane1**, **Folder1** lub **Folder2**, zaznaczone foldery zostaną uwzględnione w kopii zapasowej jako zwykłe foldery bez względu na stan opcji **Punkty zamontowania**.

5.9.14 Migawka wielowoluminowa

Ta opcja jest dostępna tylko w systemach operacyjnych Windows.

Opcja ta dotyczy kopii zapasowej na poziomie dysku. Opcja ta dotyczy również kopii zapasowej na poziomie plików, jeśli kopia zapasowa jest tworzona przez wykonanie migawki (opcja Migawka kopii zapasowej na poziomie plików (s. 61) określa, czy podczas tworzenia kopii zapasowej na poziomie plików jest wykonywana migawka).

Ta opcja określa, czy migawki kilku woluminów mają zostać utworzone jednocześnie, czy po kolei.

Ustawienie wstępne: **Włączona**.

W przypadku włączenia tej opcji migawki wszystkich woluminów uwzględnianych w kopii zapasowej są tworzone jednocześnie. Użyj tej opcji, aby utworzyć spójną czasowo kopię zapasową danych na wielu woluminach, na przykład dla bazy danych Oracle.

Jeśli ta opcja jest wyłączona, migawki woluminów są wykonywane po kolei. W rezultacie utworzona w ten sposób kopia zapasowa może nie być spójna, jeśli dane znajdują się na wielu woluminach.

5.9.15 Wydajność

Priorytet procesu

Ta opcja umożliwia określenie priorytetu procesu tworzenia kopii zapasowej w systemie operacyjnym.

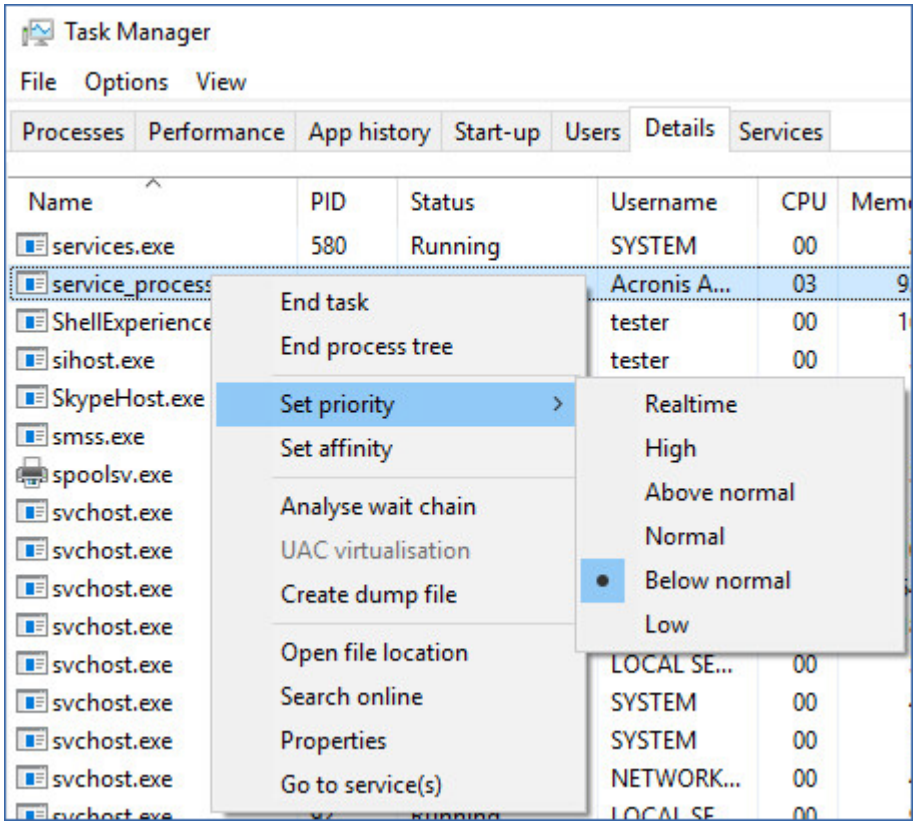
Dostępne są następujące ustawienia: **Niski**, **Normalny**, **Wysoki**.

Ustawienie wstępne: **Niski**(w systemie Windows odpowiada ustawieniu **Poniżej normalnego**).

Priorytet procesu działającego w systemie określa ilość mocy obliczeniowej procesora i zasobów systemowych przydzielonych do tego procesu. Obniżenie priorytetu tworzenia kopii zapasowej zwolni więcej zasobów dla pozostałych aplikacji. Podwyższenie priorytetu tworzenia kopii zapasowej może przyspieszyć proces tworzenia kopii zapasowej przez żądanie przydzielenia przez system operacyjny większej ilości zasobów, takich jak moc obliczeniowa procesora, aplikacji tworzącej kopię zapasową. Jednak efekt takiej operacji będzie zależał od całkowitego wykorzystania mocy obliczeniowej procesora oraz innych czynników, takich jak szybkość odczytu/zapisu na dysku czy natężenie ruchu w sieci.

Copyright © Acronis International GmbH, 2002-2017

Ta opcja umożliwia ustawienie priorytetu procesu tworzenia kopii zapasowej (**service_process.exe)** w systemie Windows oraz parametru niceness procesu tworzenia kopii zapasowej (**service_process)** w systemach Linux i OS X.



Szybkość danych wyjściowych podczas tworzenia kopii zapasowej

Ta opcja umożliwia ograniczenie szybkości zapisu na dysku twardym (gdy kopia zapasowa jest tworzona w folderze lokalnym) lub szybkości przesyłania danych kopii zapasowej przez sieć (gdy kopia zapasowa jest tworzona w udziale sieciowym lub chmurze).

Ustawienie wstępne: **Wyłączone**.

W przypadku włączenia tej opcji można określić maksymalną dozwoloną szybkość danych wyjściowych w KB/s.

5.9.16 Polecenia poprzedzające/następujące

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	Kopia zapasowa	Polecenie następujące po utworzeniu kopii zapasowej

Przykłady zastosowania poleceń poprzedzających/następujących:

- Usuwanie tymczasowych plików z dysku przed rozpoczęciem tworzenia kopii zapasowej.
- Konfigurowanie uruchamiania programu antywirusowego innego producenta przed każdym rozpoczęciem tworzenia kopii zapasowej.

Copyright © Acronis International GmbH, 2002-2017

- Wybiórcze kopiowanie kopii zapasowych do innej lokalizacji. Przydatność tej opcji polega na tym, że w ramach replikacji skonfigurowanej w planie tworzenia kopii zapasowych *każda* kopia zapasowa jest kopiowana do kolejnych lokalizacji.

Agent przeprowadza replikację *po* wykonaniu polecenia następującego po utworzeniu kopii zapasowej.

Program nie obsługuje poleceń interaktywnych wymagających wpisania tekstu przez użytkownika (na przykład „pause”).

5.9.16.1 Polecenie poprzedzające utworzenie kopii zapasowej

Aby określić polecenie/plik wsadowy do wykonania przed rozpoczęciem procesu tworzenia kopii zapasowej

1. Włącz przełącznik **Wykonaj polecenie przed utworzeniem kopii zapasowej**.
2. W polu **Polecenie** wpisz polecenie lub wyszukaj plik wsadowy. Program nie obsługuje poleceń interaktywnych, czyli wymagających wpisania tekstu przez użytkownika (na przykład „pause”).
3. W polu **Katalog roboczy** określ ścieżkę katalogu, w którym zostanie wykonane polecenie lub plik wsadowy.
4. W polu **Argumenty** w razie potrzeby określ argumenty wykonywania polecenia.
5. W zależności od wyniku, który chcesz uzyskać, wybierz odpowiednie opcje opisane w poniższej tabeli.
6. Kliknij **Gotowe**.

Pole wyboru	**Wybór**			
Jeśli wykonanie polecenia się nie powiedzie, zakończ tworzenie kopii zapasowej niepowodzeniem*	Wybrane	Niewybrane	Wybrane	Niewybrane
Nie twórz kopii zapasowej przed zakończeniem wykonywania polecenia	Wybrane	Wybrane	Niewybrane	Niewybrane
Wynik				
	Ustawienie wstępne Utwórz kopię zapasową dopiero po pomyślnym wykonaniu polecenia. Jeśli wykonanie polecenia się nie powiedzie, zakończ tworzenie kopii zapasowej niepowodzeniem.	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 uznaje się za niewykonane, jeśli jego kod zakończenia jest różny od zera.

Copyright © Acronis International GmbH, 2002-2017

5.9.16.2 Polecenie następujące po utworzeniu kopii zapasowej

Aby określić polecenie/plik wykonywalny, które mają zostać wykonane po zakończeniu tworzenia kopii zapasowej

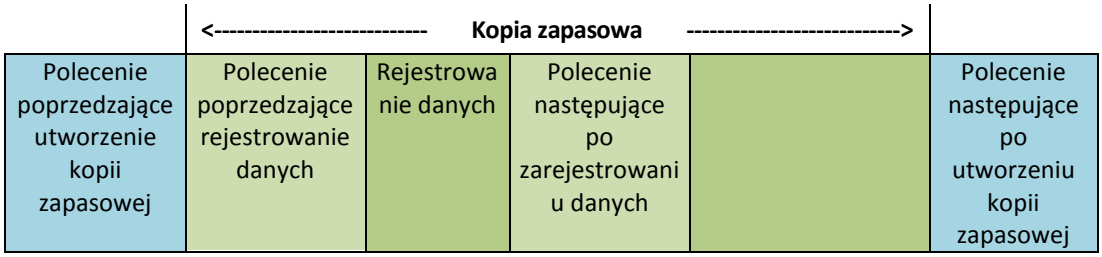
1. Włącz przełącznik **Wykonaj polecenie po utworzeniu kopii zapasowej**.
2. W polu **Polecenie** wpisz polecenie lub wyszukaj plik wsadowy.
3. W polu **Katalog roboczy** określ ścieżkę katalogu, w którym zostanie wykonane polecenie lub plik wsadowy.
4. W polu **Argumenty** w razie potrzeby określ argumenty wykonywania polecenia.
5. Jeśli pomyślne wykonanie polecenia ma znaczenie krytyczne, zaznacz pole wyboru **Jeśli wykonanie polecenia się nie powiedzie, zakończ tworzenie kopii zapasowej niepowodzeniem**. Polecenie uznaje się za niewykonane, jeśli jego kod zakończenia jest różny od zera. W takim przypadku kopia zapasowa będzie miała ustawiony status **Błąd**.

   Jeśli to pole wyboru nie jest zaznaczone, wynik wykonania polecenia nie wpływa na powodzenie lub niepowodzenie operacji tworzenia kopii zapasowej. Wynik wykonania polecenia można sprawdzić, przeglądając kartę **Działania**.
6. Kliknij **Gotowe**.

5.9.17 Polecenia poprzedzające rejestrowanie danych/następujące po nim

Ta opcja umożliwia określenie poleceń wykonywanych automatycznie przed zarejestrowaniem danych i po jego zakończeniu (czyli wykonaniu migawki danych). Dane są rejestrowane na początku procedury tworzenia kopii zapasowej.

Poniższy schemat przedstawia czas wykonania poleceń poprzedzających i następujących po rejestrowaniu danych.



Jeśli opcja (s. 70) Usługa kopiowania woluminów w tle jest włączona, wykonywanie poleceń i czynności usługi Microsoft VSS odbędzie się w następującej kolejności:

Polecenia „Przed zarejestrowaniem danych” -> Wstrzymanie VSS -> Zarejestrowanie danych -> Wznowienie VSS -> Polecenia „Po zarejestrowaniu danych”.

Przy użyciu poleceń wykonywanych przed rejestrowaniem danych/następujących po nim można zawiesić lub wznowić działanie bazy danych lub aplikacji, która nie jest kompatybilna z usługą VSS. Ponieważ rejestracja danych trwa raptem kilka sekund, czas bezczynności baz danych lub aplikacji będzie naprawdę minimalny.

5.9.17.1 Polecenie poprzedzające rejestrowanie danych

Aby określić polecenie/plik wsadowy do wykonania przed rozpoczęciem procesu rejestrowania danych

1. Włącz przełącznik **Wykonaj polecenie przed zarejestrowaniem danych**.

Copyright © Acronis International GmbH, 2002-2017

2. W polu **Polecenie** wpisz polecenie lub wyszukaj plik wsadowy. Program nie obsługuje poleceń interaktywnych, czyli wymagających wpisania tekstu przez użytkownika (na przykład „pause”).
3. W polu **Katalog roboczy** określ ścieżkę katalogu, w którym zostanie wykonane polecenie lub plik wsadowy.
4. W polu **Argumenty** w razie potrzeby określ argumenty wykonywania polecenia.
5. W zależności od wyniku, który chcesz uzyskać, wybierz odpowiednie opcje opisane w poniższej tabeli.
6. Kliknij **Gotowe**.

Pole wyboru	**Wybór**			
Jeśli wykonanie polecenia się nie powiedzie, zakończ tworzenie kopii zapasowej niepowodzeniem*	Wybrane	Niewybrane	Wybrane	Niewybrane
Nie rejestruj danych przed zakończeniem wykonywania polecenia	Wybrane	Wybrane	Niewybrane	Niewybrane
Wynik				
	Ustawienie wstępne Zarejestruj dane dopiero po pomyślnym wykonaniu polecenia. Jeśli wykonanie polecenia się nie powiedzie, zakończ tworzenie kopii zapasowej niepowodzeniem.	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 uznaje się za niewykonane, jeśli jego kod zakończenia jest różny od zera.

5.9.17.2 Polecenie następujące po zarejestrowaniu danych

Aby określić polecenie/plik wsadowy do wykonania po zarejestrowaniu danych

1. Włącz przełącznik **Wykonaj polecenie po zarejestrowaniu danych**.
2. W polu **Polecenie** wpisz polecenie lub wyszukaj plik wsadowy. Program nie obsługuje poleceń interaktywnych, czyli wymagających wpisania tekstu przez użytkownika (na przykład „pause”).
3. W polu **Katalog roboczy** określ ścieżkę katalogu, w którym zostanie wykonane polecenie lub plik wsadowy.
4. W polu **Argumenty** w razie potrzeby określ argumenty wykonywania polecenia.
5. W zależności od wyniku, który chcesz uzyskać, wybierz odpowiednie opcje opisane w poniższej tabeli.
6. Kliknij **Gotowe**.

Pole wyboru	**Wybór**			
Jeśli wykonanie polecenia się nie powiedzie, zakończ tworzenie kopii zapasowej niepowodzeniem*	Wybrane	Niewybrane	Wybrane	Niewybrane

Copyright © Acronis International GmbH, 2002-2017

Nie twórz kopii zapasowej przed zakończeniem wykonywania polecenia	Wybrane	Wybrane	Niewybrane	Niewybrane
Wynik				
	Ustawienie wstępne Kontynuuj tworzenie kopii zapasowej dopiero po pomyślnym wykonaniu polecenia.	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.

* Polecenie uznaje się za niewykonane, jeśli jego kod zakończenia jest różny od zera.

5.9.18 Tworzenie harmonogramu

Ta opcja umożliwia określenie, czy tworzenie kopii zapasowych ma się rozpoczynać zgodnie z harmonogramem, czy z opóźnieniem, a także określenie liczby maszyn wirtualnych uwzględnianych jednocześnie w kopii zapasowej.

Ustawienie wstępne:

- Wdrożenie lokalne: **Rozpocznij wszystkie operacje tworzenia kopii zapasowych dokładnie według harmonogramu.**
- Wdrożenie chmurowe: **Rozłóż uruchamianie operacji tworzenia kopii zapasowych w przedziale czasu. Maksymalne opóźnienie: 30 minut.**

Możesz wybrać jedną z następujących opcji:

- **Rozpocznij wszystkie operacje tworzenia kopii zapasowych dokładnie według harmonogramu**

  Tworzenie kopii zapasowych komputerów fizycznych będzie się rozpoczynać zgodnie z harmonogramem. Kopie zapasowe maszyn wirtualnych będą tworzone pojedynczo.
- **Rozłóż uruchamianie w przedziale czasu**

  Tworzenie kopii zapasowych komputerów fizycznych będzie się rozpoczynać z opóźnieniem w stosunku do zaplanowanego czasu. Wartość opóźnienia jest w przypadku każdego komputera wybierana losowo i mieści się w zakresie od zera do określonej przez Ciebie wartości maksymalnej. Ustawienia tego warto użyć w przypadku tworzenia kopii zapasowych wielu komputerów w lokalizacji sieciowej — pozwoli ono uniknąć nadmiernego obciążenia sieci. Wartość opóźnienia dla poszczególnych komputerów jest ustalana podczas stosowania planu tworzenia kopii zapasowych na tych komputerach. Pozostaje ona niezmienna do chwili ewentualnej edycji planu i zmiany maksymalnej wartości opóźnienia.

  Kopie zapasowe maszyn wirtualnych będą tworzone pojedynczo.
- **Ogranicz liczbę jednoczesnych operacji tworzenia kopii zapasowych o**

  Ta opcja jest dostępna tylko wtedy, gdy plan tworzenia kopii zapasowych jest stosowany do wielu maszyn wirtualnych. Określa ona liczbę maszyn wirtualnych, których kopie zapasowe agent może utworzyć jednocześnie podczas wykonywania danego planu tworzenia kopii zapasowych.

  Jeśli zgodnie z planem tworzenia kopii zapasowych agent ma rozpocząć jednoczesne tworzenie kopii wielu maszyn, wybierze on dwie maszyny (w celu optymalizacji wydajności tworzenia kopii zapasowych agent próbuje dopasować maszyny przechowywane w różnych pamięciach

Copyright © Acronis International GmbH, 2002-2017

masowych). Po zakończeniu tworzenia dwóch kopii zapasowych agent wybierze kolejną maszynę itd.

Program umożliwia zmianę liczby maszyn wirtualnych, których kopie zapasowe agent tworzy jednocześnie. Wartością maksymalną jest 10.

Tworzenie kopii zapasowych komputerów fizycznych będzie się rozpoczynać zgodnie z harmonogramem.

5.9.19 Kopia zapasowa sektor po sektorze

Ta opcja jest dostępna tylko w przypadku kopii zapasowych na poziomie dysku.

Opcja umożliwia określenie, czy ma zostać utworzona dokładna kopia dysku lub woluminu na poziomie fizycznym.

Ustawienie wstępne: **Wyłączone**.

W przypadku włączenia tej opcji w kopii zapasowej zostaną uwzględnione wszystkie sektory dysku lub woluminu, w tym nieprzydzielone miejsce oraz sektory bez danych. Wynikowa kopia zapasowa będzie tego samego rozmiaru co uwzględniany w niej dysk (jeśli opcja „Stopień kompresji” (s. 58) ma wartość **Brak**). W przypadku tworzenia kopii zapasowej dysków z nierozpoznanym lub nieobsługiwanym systemem plików oprogramowanie automatycznie przełącza się na tryb „sektor po sektorze”.

5.9.20 Dzielenie

Ta opcja jest dostępna w przypadku schematów tworzenia kopii zapasowych **Zawsze pełne**; **Tygodniowe pełne, dzienne przyrostowe** oraz **Niestandardowy**.

Opcja umożliwia wybranie metody dzielenia dużych kopii zapasowych na mniejsze pliki.

Ustawienie wstępne: **Automatycznie**.

Dostępne są poniższe ustawienia:

- **Automatycznie**

  Jeśli rozmiar kopii zapasowej przekroczy maksymalny rozmiar pliku obsługiwany przez dany system plików, kopia zapasowa zostanie podzielona.
- **Stały rozmiar**

  Wprowadź wymagany rozmiar pliku lub wybierz go z listy rozwijanej.

5.9.21 Obsługa niepowodzenia zadania

Ta opcja określa zachowanie programu, jeśli nie uda się wykonać planu tworzenia kopii zapasowych.

W przypadku włączenia tej opcji program jeszcze raz spróbuje wykonać plan tworzenia kopii zapasowych. Można określić liczbę prób oraz odstępy 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.

Ustawienie wstępne: **Wyłączone**.

5.9.22 Usługa kopiowania woluminów w tle (VSS)

Ta opcja jest dostępna tylko w systemach operacyjnych Windows.

Copyright © Acronis International GmbH, 2002-2017

Określa ona, czy dostawca Usługi kopiowania woluminów w tle (VSS) ma powiadamiać aplikacje obsługujące technologię VSS o planowanym 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 danych przez oprogramowanie do tworzenia kopii zapasowych. Spójność danych zapewnia z kolei możliwość odzyskania aplikacji w prawidłowym stanie i umożliwia rozpoczęcie jej używania natychmiast po odzyskaniu.

Ustawienie wstępne: **Włączona**. **Automatycznie wybierz dostawcę migawek**.

Możesz wybrać jedną z następujących opcji:

- **Automatycznie wybierz dostawcę migawek**

  Automatycznie wybierz między sprzętowym dostawcą migawek, programowymi dostawcami migawek a Dostawcą kopiowania w tle oprogramowania firmy Microsoft.
- **Użyj Dostawcy kopiowania w tle oprogramowania firmy Microsoft**

  Zaleca się wybór tej opcji w przypadku tworzenia kopii zapasowych serwerów aplikacji (Microsoft Exchange Server, Microsoft SQL Server, Microsoft SharePoint lub Active Directory).

Jeśli baza danych jest niekompatybilna z usługą VSS, wyłącz tę opcję. Migawki są tworzone szybciej, ale nie można zagwarantować spójności danych aplikacji, których transakcje nie zostały zakończone do czasu wykonania migawki. Aby zapewnić spójność danych uwzględnianych w kopii zapasowej, można użyć poleceń poprzedzających rejestrowanie danych/następujących po nim (s. 67). 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.

Włącz tworzenie pełnych kopii zapasowych z usługą VSS

Jeśli ta opcja jest włączona, dzienniki programu Microsoft Exchange Server i innych aplikacji uwzględniających usługę VSS (z wyjątkiem programu Microsoft SQL Server) będą obcinane po każdym pomyślnym utworzeniu pełnej, przyrostowej lub różnicowej kopii zapasowej na poziomie dysku.

Ustawienie wstępne: **Wyłączone**.

Opcja ta powinna być wyłączona w następujących przypadkach:

- Jeśli do tworzenia kopii zapasowych danych programu Exchange Server jest używany agent dla programu Exchange lub program innego producenta. W takim przypadku obcinanie dziennika będzie wpływało na kolejne kopie zapasowe dziennika transakcji.
- Jeśli do tworzenia kopii zapasowych danych serwera SQL jest używany program innego producenta. Wynika to z faktu, że program innego producenta uzna wynikową kopię zapasową na poziomie dysku za „własną” pełną kopię. Dlatego utworzenie kolejnej różnicowej kopii zapasowej danych serwera SQL zakończy się niepowodzeniem. Tworzenie kopii zapasowych będzie kończyło się niepowodzeniem do czasu, aż program innego producenta utworzy kolejną „własną” pełną kopię zapasową.
- Jeśli na komputerze są uruchomione inne aplikacje uwzględniające usługę VSS i z jakiegoś powodu chcesz zachować ich dzienniki.

Włączenie tej opcji nie powoduje obcinania dzienników programu Microsoft SQL Server. Aby dziennik programu SQL Server był obcinany po utworzeniu kopii zapasowej, włącz opcję tworzenia kopii zapasowych Obcinanie dziennika (s. 62).

 Copyright © Acronis International GmbH, 2002-2017

5.9.23 Usługa kopiowania woluminów w tle (VSS) dla maszyn wirtualnych

Opcja umożliwia określenie, czy są wykonywane wyciszone migawki maszyny wirtualnej. Aby wykonać wyciszoną migawkę, oprogramowanie do tworzenia kopii zapasowych stosuje usługę VSS w ramach maszyny wirtualnej, korzystając z narzędzi VMware Tools lub usług integracji Hyper-V.

Ustawienie wstępne: **Włączona**.

W przypadku włączenia tej opcji transakcje wszystkich aplikacji uwzględniających usługę VSS działające na maszynie wirtualnej zostaną ukończone przed wykonaniem migawki. Jeśli po określonej w opcji „Obsługa błędów” (s. 59) liczbie prób nie uda się utworzyć wyciszonej migawki i jest wyłączone tworzenie kopii zapasowych aplikacji, zostanie wykonana niewyciszona migawka. Jeśli tworzenie kopii zapasowych aplikacji jest włączone, tworzenie kopii zapasowej zakończy się niepowodzeniem.

W przypadku wyłączenia tej opcji wykonywana jest niewyciszona migawka. Maszyna wirtualna zostanie uwzględniona w kopii zapasowej w stanie spójności po awarii.

5.9.24 Tygodniowa kopia zapasowa

Ta opcja umożliwia wskazanie, które kopie zapasowe należy uznać za „tygodniowe” w regułach przechowywania i schematach tworzenia kopii zapasowych. „Tygodniową” kopią zapasową jest pierwsza kopia zapasowa utworzona po rozpoczęciu tygodnia.

Ustawienie wstępne: **Poniedziałek**.

5.9.25 Dziennik zdarzeń systemu Windows

Ta opcja jest dostępna tylko w systemach operacyjnych Windows.

Opcja umożliwia określenie, czy agenty muszą rejestrować zdarzenia operacji tworzenia kopii zapasowych w dzienniku zdarzeń aplikacji systemu Windows (aby wyświetlić ten dziennik, uruchom plik eventvwr.exe lub wybierz **Panel sterowania** > **Narzędzia administracyjne** > **Podgląd zdarzeń**). Zdarzenia, które mają być rejestrowane, można filtrować.

Ustawienie wstępne: **Wyłączone**.

6 Odzyskiwanie

6.1 Odzyskiwanie — ściągawka

W poniższej tabeli zestawiono dostępne metody odzyskiwania. Dzięki niej wybierzesz optymalną metodę odzyskiwania.

Elementy do odzyskania	Metoda odzyskiwania
Komputer fizyczny (z systemem Windows lub Linux)	Przy użyciu interfejsu internetowego (s. 74) Przy użyciu nośnika startowego (s. 78)
Komputer fizyczny (z systemem Mac)	Przy użyciu nośnika startowego (s. 78)

Copyright © Acronis International GmbH, 2002-2017

Maszyna wirtualna (VMware lub Hyper-V)	Przy użyciu interfejsu internetowego (s. 76) Przy użyciu nośnika startowego (s. 78)
Konfiguracja ESXi	Przy użyciu nośnika startowego (s. 85)
Pliki/foldery	Przy użyciu interfejsu internetowego (s. 82) Pobieranie plików z chmury (s. 83) Przy użyciu nośnika startowego (s. 84) Wyodrębnianie plików z lokalnych kopii zapasowych (s. 84)
Stan systemu	Przy użyciu interfejsu internetowego (s. 85)
Bazy danych SQL	Przy użyciu interfejsu internetowego (s. 113)
Bazy danych programu Exchange	Przy użyciu interfejsu internetowego (s. 116)
Skrzynki pocztowe programu Exchange	Przy użyciu interfejsu internetowego (s. 117)
Skrzynki pocztowe Office 365	Przy użyciu interfejsu internetowego (s. 122)

Uwaga dla użytkowników komputerów Mac

- Począwszy od wersji 10.11 El Capitan, niektóre pliki systemowe, foldery i procesy są oflagowane do ochrony przy użyciu rozszerzonego atrybutu pliku com.apple.rootless. Funkcja ta jest nazywana ochroną integralności systemu (System Integrity Protection, SIP). Chronione pliki obejmują preinstalowane aplikacje oraz większość folderów w folderach /system, /bin, /sbin, /usr.

  Chronione pliki i foldery nie mogą zostać zastąpione podczas operacji odzyskiwania w ramach tego systemu operacyjnego. Jeśli zechcesz zastąpić chronione pliki, przeprowadź operację odzyskiwania przy użyciu nośnika startowego.
- Począwszy od systemu macOS Sierra 10.12, funkcja Store in Cloud może przenosić rzadko używane pliki do środowiska iCloud. W systemie plików pozostają niewielkie „odciski” tych plików i to one są uwzględniane w kopii zapasowej zamiast pierwotnych plików.

  Po odzyskaniu odcisku do oryginalnej lokalizacji jest on synchronizowany z usługą iCloud, dzięki czemu pierwotny plik staje się znów dostępny. Po odzyskaniu odcisku do innej lokalizacji nie można go zsynchronizować z usługą iCloud, wskutek czego pierwotny plik będzie niedostępny.

6.2 Tworzenie nośnika startowego

Nośnik startowy to dysk CD, DVD, flash USB lub inny nośnik wymienny, który umożliwia uruchamianie agenta bez udziału systemu operacyjnego. Głównym zastosowaniem nośnika startowego jest odzyskanie systemu operacyjnego, którego nie można uruchomić.

Zdecydowanie zaleca się utworzenie i wypróbowanie nośnika startowego natychmiast po rozpoczęciu stosowania kopii zapasowych na poziomie dysku. Warto też ponownie tworzyć nośnik po każdej istotnej aktualizacji agenta kopii zapasowych.

Jeden nośnik może służyć do odzyskania systemu Windows lub systemu Linux. Aby odzyskać system OS X, należy utworzyć osobny nośnik na komputerze z systemem OS X.

Aby utworzyć nośnik startowy w systemie Windows lub Linux

1. Pobierz plik ISO nośnika startowego. Aby pobrać ten plik, wybierz komputer i kliknij **Odzyskaj** > **Więcej metod odzyskiwania** > **Pobierz obraz ISO**.
2. Wykonaj dowolne z następujących czynności:
   - Nagraj plik ISO na dysku CD/DVD.
   - Utwórz startowy dysk flash USB przy użyciu pliku ISO i jednego z bezpłatnych narzędzi dostępnych online.

Copyright © Acronis International GmbH, 2002-2017

Użyj narzędzia `ISO to USB` lub RUFUS, jeśli chcesz uruchomić komputer z technologią UEFI, albo narzędzia `Win32DiskImager` w przypadku komputera z systemem BIOS. W systemie Linux warto skorzystać z narzędzia `dd`.

- Podłącz plik ISO jako dysk CD/DVD do maszyny wirtualnej, którą chcesz odzyskać.

Możesz też utworzyć nośnik startowy za pomocą Generatora nośnika startowego (s. 95).

Aby utworzyć nośnik startowy w systemie OS X

1. Na komputerze z zainstalowanym agentem dla systemu Mac kliknij **Aplikacje** > **Generator nośnika ratunkowego**.
2. Oprogramowanie wyświetli podłączone nośniki wymienne. Wybierz ten, który ma być nośnikiem startowym.

   Ostrzeżenie *Wszystkie dane zapisane na tym dysku zostaną skasowane.*
3. Kliknij **Utwórz**.
4. Poczekaj, aż oprogramowanie utworzy nośnik startowy.

6.3 Odzyskiwanie komputera

6.3.1 Komputer fizyczny

W tej sekcji opisano odzyskiwanie komputerów fizycznych przy użyciu interfejsu internetowego.

Czasem lepiej użyć nośnika startowego, a nie interfejsu internetowego. Dotyczy to odzyskiwania następujących elementów:

- System OS X
- Dowolny system operacyjny na komputer bez systemu operacyjnego lub komputer w trybie offline

Odzyskanie systemu operacyjnego wymaga ponownego uruchomienia systemu. Możesz określić automatyczne ponowne uruchomienie komputera lub przypisać mu status **Wymagane działanie**. Odzyskany system operacyjny automatycznie przechodzi w tryb online.

Aby odzyskać komputer fizyczny

1. Wybierz komputer uwzględniony w kopii zapasowej.
2. Kliknij **Odzyskiwanie**.
3. Wybierz punkt odzyskiwania. Uwaga: punkty odzyskiwania są filtrowane na podstawie lokalizacji.

   Jeśli komputer jest w trybie offline, punkty odzyskiwania nie są wyświetlane. Wykonaj dowolne z następujących czynności:

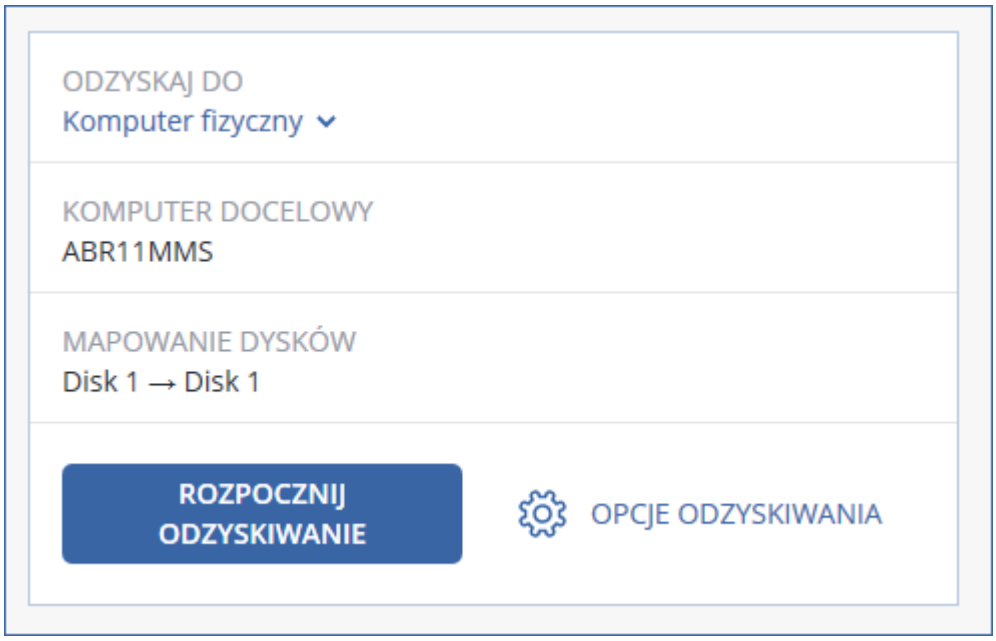
   - Jeśli lokalizacją kopii zapasowych jest chmura lub współużytkowany magazyn (czyli magazyn, do którego mają dostęp inne agenty), kliknij **Wybierz komputer**, wybierz komputer docelowy będący w trybie online i wybierz punkt odzyskiwania.
   - Wybierz punkt odzyskiwania na karcie Kopie zapasowe (s. 92).
   - Odzyskaj komputer zgodnie z instrukcjami podanymi w sekcji „Odzyskiwanie dysków przy użyciu nośnika startowego” (s. 78).
4. Kliknij **Odzyskaj** > **Cały komputer**.

   Program automatycznie zamapuje dyski z kopii zapasowej na dyski komputera docelowego.

   - Aby odzyskać na inny komputer fizyczny, kliknij **Komputer docelowy** i wybierz komputer docelowy będący w trybie online.

Copyright © Acronis International GmbH, 2002-2017

- Jeśli mapowanie dysków się nie powiedzie, odzyskaj komputer zgodnie z opisem podanym w sekcji „Odzyskiwanie dysków przy użyciu nośnika startowego” (s. 78). Skorzystanie z nośnika umożliwia wybranie dysków do odzyskania i ręczne ich zamapowanie.



5. Kliknij **Rozpocznij odzyskiwanie**.
6. Potwierdź, że chcesz zastąpić dyski ich wersjami z kopii zapasowej. Określ, czy komputer ma zostać automatycznie ponownie uruchomiony.

Postęp odzyskiwania jest widoczny na karcie **Działania**.

6.3.2 Komputer fizyczny na maszynę wirtualną

W tej sekcji opisano odzyskiwanie komputera fizycznego jako maszyny wirtualnej przy użyciu interfejsu internetowego. Operację tę można wykonać, jeśli jest zainstalowany i zarejestrowany co najmniej jeden agent dla VMware lub agent dla Hyper-V.

Więcej informacji na temat migracji komputera fizycznego na maszynę wirtualną (P2V) można znaleźć w sekcji „Migracja komputera” (s. 131).

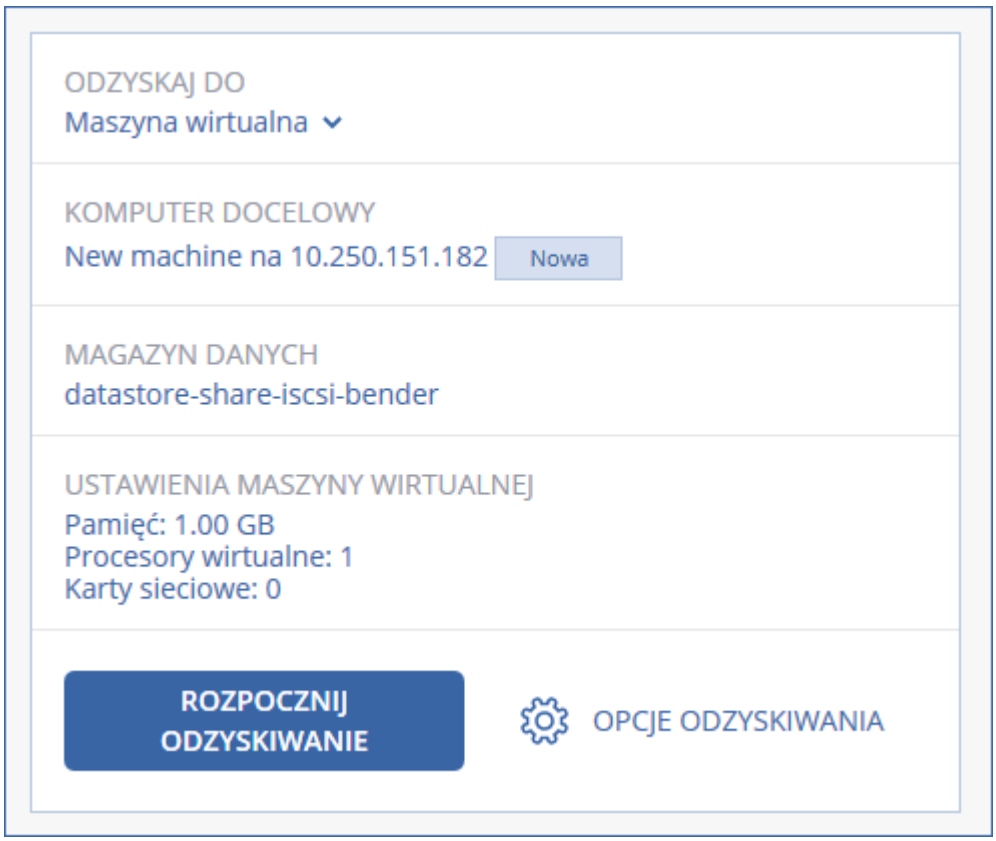
Aby odzyskać komputer fizyczny jako maszynę wirtualną

1. Wybierz komputer uwzględniony w kopii zapasowej.
2. Kliknij **Odzyskiwanie**.
3. Wybierz punkt odzyskiwania. Uwaga: punkty odzyskiwania są filtrowane na podstawie lokalizacji.

   Jeśli komputer jest w trybie offline, punkty odzyskiwania nie są wyświetlane. Wykonaj dowolne z następujących czynności:
   - Jeśli lokalizacją kopii zapasowych jest chmura lub współużytkowany magazyn (czyli magazyn, do którego mają dostęp inne agenty), kliknij **Wybierz komputer**, wybierz komputer będący w trybie online i wybierz punkt odzyskiwania.
   - Wybierz punkt odzyskiwania na karcie Kopie zapasowe (s. 92).
   - Odzyskaj komputer zgodnie z instrukcjami podanymi w sekcji „Odzyskiwanie dysków przy użyciu nośnika startowego” (s. 78).
4. Kliknij **Odzyskaj** > **Cały komputer**.
5. W polu **Odzyskaj do** wybierz **Maszyna wirtualna**.

Copyright © Acronis International GmbH, 2002-2017

6. Kliknij **Komputer docelowy**.
   a. Wybierz hiperwizor (**VMware ESXi** lub **Hyper-V**).
      Musi być zainstalowany co najmniej jeden agent dla VMware lub agent dla Hyper-V.
   b. Określ, czy chcesz odzyskać na nową, czy na już istniejącą maszyną wirtualną. Lepsza jest opcja nowej maszyny, ponieważ nie wymaga, aby konfiguracja dysków maszyny docelowej była dokładnie taka sama jak konfiguracja dysków w kopii zapasowej.
   c. Wybierz host i określ nazwę nowej maszyny lub wybierz istniejącą maszynę docelową.
   d. Kliknij **OK**.
7. [Opcjonalnie] W przypadku odzyskiwania na nową maszynę możesz też wykonać następujące czynności:
   - Kliknij **Magazyn danych** w przypadku ESXi lub **Ścieżka** w przypadku Hyper-V, a następnie wybierz magazyn danych (magazyn) dla maszyny wirtualnej.
   - Kliknij **Ustawienia maszyny wirtualnej**, aby zmienić rozmiar pamięci, liczbę procesorów oraz połączenia sieciowe maszyny wirtualnej.



8. Kliknij **Rozpocznij odzyskiwanie**.
9. W przypadku odzyskiwania na istniejącą maszynę wirtualną potwierdź, że chcesz zastąpić dyski.

Postęp odzyskiwania jest widoczny na karcie **Działania**.

6.3.3 Maszyna wirtualna

Podczas odzyskiwania maszyna wirtualna nie może działać. Oprogramowanie zatrzyma maszynę bez wyświetlenia monitu. Po zakończeniu odzyskiwania trzeba będzie ręcznie uruchomić maszynę.

To zachowanie można zmienić za pomocą opcji odzyskiwania służącej do zarządzania zasilaniem maszyn wirtualnych (kliknij **Opcje odzyskiwania** > **Zarządzanie zasilaniem maszyn wirtualnych**).

Copyright © Acronis International GmbH, 2002-2017

Aby odzyskać maszynę wirtualną

1. Wykonaj jedną z następujących czynności:
   - Wybierz komputer uwzględniony w kopii zapasowej, kliknij **Odzyskaj**, a następnie wybierz punkt odzyskiwania.
   - Wybierz punkt odzyskiwania na karcie Kopie zapasowe (s. 92).
2. Kliknij **Odzyskaj** > **Cały komputer**.
3. Jeśli chcesz odzyskać na komputer fizyczny, wybierz **Komputer fizyczny** w polu **Odzyskaj do**. W przeciwnym razie pomiń ten krok.

   Odzyskanie na komputer fizyczny jest możliwe pod warunkiem, że konfiguracja dysków komputera docelowego jest dokładnie taka sama jak konfiguracja dysków w kopii zapasowej.

   Jeśli tak jest, przejdź do kroku 4 w sekcji „Komputer fizyczny” (s. 74). W przeciwnym wypadku najlepiej przeprowadź migrację maszyny wirtualnej na komputer fizyczny (V2P) przy użyciu nośnika startowego (s. 78).
4. Program automatycznie wybierze pierwotny komputer jako komputer docelowy.

   Aby odzyskać na inną maszynę wirtualną, kliknij **Komputer docelowy**, a następnie zrób tak:

   a. Wybierz hiperwizor (**VMware ESXi** lub **Hyper-V**).

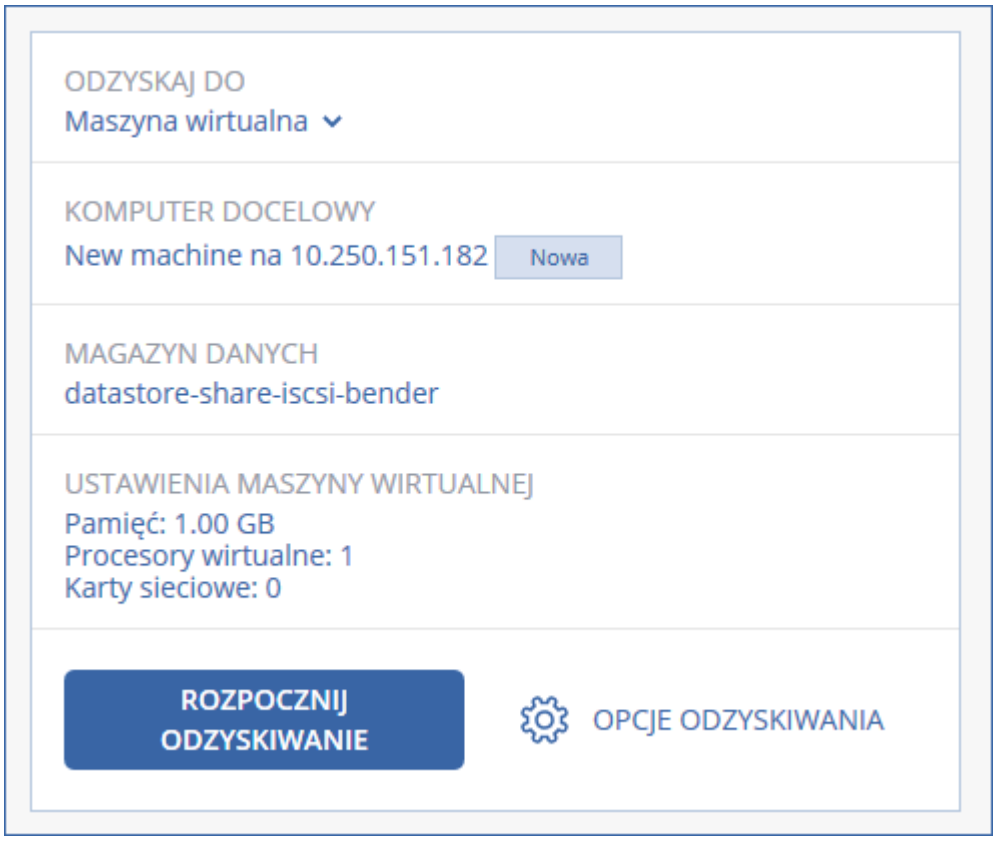
   b. Określ, czy chcesz odzyskać na nową, czy na już istniejącą maszyną wirtualną.

   c. Wybierz host i określ nazwę nowej maszyny lub wybierz istniejącą maszynę docelową.

   d. Kliknij **OK**.
5. [Opcjonalnie] W przypadku odzyskiwania na nową maszynę możesz też wykonać następujące czynności:
   - Kliknij **Magazyn danych** w przypadku ESXi lub **Ścieżka** w przypadku Hyper-V, a następnie wybierz magazyn danych (magazyn) dla maszyny wirtualnej.

Copyright © Acronis International GmbH, 2002-2017

- Kliknij **Ustawienia maszyny wirtualnej**, aby zmienić rozmiar pamięci, liczbę procesorów oraz połączenia sieciowe maszyny wirtualnej.



6. Kliknij **Rozpocznij odzyskiwanie**.
7. W przypadku odzyskiwania na istniejącą maszynę wirtualną potwierdź, że chcesz zastąpić dyski.

Postęp odzyskiwania jest widoczny na karcie **Działania**.

6.3.4 Odzyskiwanie dysków przy użyciu nośnika startowego

Informacje na temat tworzenia nośnika startowego można znaleźć w sekcji „Tworzenie nośnika startowego” (s. 73).

Aby odzyskać dyski przy użyciu nośnika startowego

1. Uruchom komputer docelowy, korzystając z nośnika startowego.
2. Kliknij **Zarządzaj tym komputerem lokalnie** lub kliknij **Ratunkowy nośnik startowy** dwa razy, w zależności od typu używanego nośnika.
3. Jeśli w danej sieci jest włączony serwer proxy, kliknij **Narzędzia** > **Serwer proxy**, a następnie określ nazwę hosta / adres IP oraz port serwera proxy. W przeciwnym razie pomiń ten krok.
4. Na ekranie powitalnym kliknij **Odzyskaj**.
5. Kliknij **Wybierz dane**, a następnie kliknij **Przeglądaj**.
6. Określ lokalizację kopii zapasowej:
   - Aby odzyskać z chmury, wybierz **Chmura**. Wprowadź poświadczenia konta, do którego jest przypisany komputer uwzględniony w kopii zapasowej.
   - Aby odzyskać z folderu lokalnego lub sieciowego, przejdź do niego w obszarze **Foldery lokalne** lub **Foldery sieciowe**.

   Kliknij **OK**, aby zatwierdzić wybór.

Copyright © Acronis International GmbH, 2002-2017

7. Wybierz kopię zapasową, z której chcesz odzyskać dane. Jeśli pojawi się monit, wpisz hasło kopii zapasowej.
8. W polu **Zawartość kopii zapasowej** wybierz dyski, które chcesz odzyskać. Kliknij **OK**, aby zatwierdzić wybór.
9. W obszarze **Lokalizacja odzyskiwania** oprogramowanie automatycznie zamapuje wybrane dyski na dyski docelowe.

   Jeśli mapowanie się nie powiedzie lub będzie niezgodne z oczekiwaniami, należy zamapować dyski ręcznie.

   Zmiana układu dysków może uniemożliwić uruchomienie systemu operacyjnego. Najlepiej użyć układu dysków pierwotnego komputera, chyba że ma się pewność udanej operacji.
10. [W przypadku odzyskiwania systemu Linux] Jeśli komputer uwzględniony w kopii zapasowej ma woluminy logiczne i chcesz odtworzyć ich pierwotną strukturę:
    a. Upewnij się, że liczba i pojemność dysków w komputerze docelowym są takie same lub większe niż liczba i pojemność dysków w pierwotnym komputerze, a następnie kliknij **Zastosuj RAID/LVM**.
    b. Zapoznaj się ze strukturą woluminów, a następnie utwórz ją, klikając **Zastosuj RAID/LVM**.
11. [Opcjonalnie] Kliknij **Opcje odzyskiwania**, aby określić dodatkowe ustawienia.
12. Kliknij **OK**, aby rozpocząć odzyskiwanie.

6.3.5 Używanie funkcji Universal Restore

Najnowsze systemy operacyjne można uruchamiać po odzyskaniu w innej konfiguracji sprzętowej, w tym na platformach VMware bądź Hyper-V. Jeśli odzyskany system operacyjny się nie uruchamia, należy za pomocą narzędzia Universal Restore zaktualizować sterowniki i moduły, które mają zasadnicze znaczenie dla uruchamiania systemu operacyjnego.

Narzędzie Universal Restore można stosować w odniesieniu do systemów Windows oraz Linux.

Aby zastosować narzędzie Universal Restore

1. Uruchom komputer za pomocą nośnika startowego.
2. Kliknij **Zastosuj funkcję Universal Restore**.
3. Jeśli na komputerze jest więcej niż jeden system operacyjny, wybierz ten z nich, w którym chcesz zastosować narzędzie Universal Restore.
4. [Tylko w systemie Windows] Skonfiguruj dodatkowe ustawienia (s. 79).
5. Kliknij **OK**.

6.3.5.1 Narzędzie Universal Restore w systemie Windows

Przygotowanie

Przygotuj sterowniki

Przed zastosowaniem narzędzia Universal Restore w systemie operacyjnym Windows sprawdź, czy masz sterowniki dla nowego kontrolera dysku twardego i chipsetu. Te sterowniki mają zasadnicze znaczenie dla uruchamiania systemu operacyjnego. Użyj płyty CD lub DVD dostarczonej przez dostawcę sprzętu lub pobierz sterowniki z witryny internetowej dostawcy. Pliki sterowników powinny mieć rozszerzenie *.inf. Jeśli pobrano sterowniki w formacie exe, cab lub zip, trzeba je wyodrębnić za pomocą aplikacji innej firmy.

Copyright © Acronis International GmbH, 2002-2017

Sprawdzoną praktyką jest przechowywanie sterowników dla całego sprzętu używanego w organizacji w jednym repozytorium, posortowanym według typu urządzenia lub według konfiguracji sprzętu. Kopię tego repozytorium można przechowywać na płycie DVD lub dysku flash, a wybrane z niego sterowniki można umieścić na nośniku startowym, tworząc niestandardowy nośnik startowy zawierający niezbędne sterowniki (oraz niezbędną konfigurację sieciową) dla każdego z używanych serwerów. Można także po prostu określać ścieżkę do repozytorium za każdym razem, gdy używane jest narzędzie Universal Restore.

Sprawdź dostęp do sterowników w środowisku startowym

Upewnij się, że masz dostęp do urządzenia ze sterownikami podczas pracy z nośnikiem startowym. Użyj nośnika opartego na środowisku WinPE, jeśli urządzenie jest dostępne w systemie Windows, ale nie wykrywa go nośnik oparty na systemie Linux.

Ustawienia narzędzia Universal Restore

Automatyczne wyszukiwanie sterowników

Określ miejsce, w którym program będzie wyszukiwać sterowników warstwy abstrakcji sprzętu (HAL), kontrolera dysku twardego i adapterów sieciowych:

- Jeśli sterowniki znajdują się na płycie lub innym nośniku wymiennym udostępnionym przez dostawcę, włącz opcję **Przeszukaj nośnik wymienny**.
- Jeśli sterowniki znajdują się w folderze sieciowym lub na nośniku startowym, określ ścieżkę do tego folderu, klikając **Dodaj folder**.

Oprócz tego narzędzie Universal Restore przeszuka domyślny folder magazynu sterowników Windows. Jego lokalizacja jest ustalona za pomocą wartości rejestru **DevicePath**, która znajduje się w kluczu rejestru **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion**. Zazwyczaj jest to folder WINDOWS/inf.

Narzędzie Universal Restore przeprowadzi rekurencyjne wyszukiwanie we wszystkich podfolderach określonego folderu, znajdzie najbardziej odpowiednie sterowniki warstwy abstrakcji sprzętu (HAL) i kontrolera dysku twardego spośród dostępnych, a następnie zainstaluje je w systemie. Narzędzie Universal Restore wyszukuje także sterownik karty sieciowej, po czym przekazuje ścieżkę znalezionego sterownika do systemu operacyjnego. Jeśli komputer jest wyposażony w kilka kart interfejsu sieciowego, narzędzie Universal Restore próbuje skonfigurować sterowniki wszystkich kart.

Sterowniki pamięci masowej do zainstalowania mimo to

Ustawienie to jest niezbędne, gdy:

- Komputer jest wyposażony w określony kontroler pamięci masowej, taki jak adapter RAID (w szczególności NVIDIA RAID) lub Fibre Channel.
- Przeprowadzona została migracja do maszyny wirtualnej, w której używany jest kontroler dysku twardego SCSI. Należy korzystać ze sterowników SCSI dołączonych do oprogramowania do wirtualizacji lub pobrać najnowsze wersje sterowników z witryny internetowej producenta oprogramowania.
- Jeśli automatyczne wyszukiwanie sterowników nie ułatwia uruchomienia systemu.

Określ odpowiednie sterowniki, klikając **Dodaj sterownik**. Zdefiniowane tutaj sterowniki zostaną zainstalowane, z odpowiednimi ostrzeżeniami, nawet gdy program znajdzie lepsze.

Działanie narzędzia Universal Restore

Po określeniu wymaganych ustawień kliknij **OK**.

Copyright © Acronis International GmbH, 2002-2017

Jeśli narzędzie Universal Restore nie znajdzie kompatybilnego sterownika w określonych lokalizacjach, wyświetli monit informujący o problemie z urządzeniem. Wykonaj jedną z następujących czynności:

- Dodaj sterownik do dowolnej z określonych wcześniej lokalizacji i kliknij **Spróbuj ponownie**.
- Jeżeli nie pamiętasz lokalizacji, kliknij **Ignoruj**, aby kontynuować proces. Jeśli wynik będzie niezadowalający, ponownie zastosuj narzędzie Universal Restore. Podczas konfigurowania operacji określ niezbędny sterownik.

Po uruchomieniu system Windows zainicjuje standardową procedurę instalowania nowego sprzętu. Sterownik adaptera sieciowego zostanie zainstalowany dyskretnie, jeśli posiada sygnaturę systemu Microsoft Windows. W przeciwnym razie system Windows poprosi o potwierdzenie zainstalowania niepodpisanego sterownika.

Po wykonaniu tych czynności można skonfigurować połączenie sieciowe i określić sterowniki adaptera wideo, USB oraz innych urządzeń.

6.3.5.2 Narzędzie Universal Restore w systemie Linux

Narzędzie Universal Restore można stosować w systemach operacyjnych Linux z jądrem w wersji 2.6.8 lub nowszej.

W przypadku zastosowania w systemie operacyjnym Linux narzędzie Universal Restore aktualizuje tymczasowy system plików określany jako początkowy dysk RAM (initrd). Pozwala to na uruchomienia systemu operacyjnego na nowym sprzęcie.

Narzędzie Universal Restore dodaje do początkowego dysku RAM moduły odpowiedzialne za nowy sprzęt (w tym sterowniki urządzeń). Na ogół niezbędne moduły znajdują się w katalogu **/lib/modules**. Gdy narzędzie Universal Restore nie może znaleźć potrzebnego modułu, rejestruje nazwę pliku modułu w dzienniku.

Narzędzie Universal Restore może modyfikować konfigurację programu startowego GRUB. Może to być wymagane na przykład w celu zapewnienia możliwości uruchomienia systemu, gdy układ woluminów na nowym komputerze różni się od układu na komputerze pierwotnym.

Narzędzie Universal Restore nigdy nie modyfikuje jądra systemu Linux.

Przywrócenie oryginalnego początkowego dysku RAM

W razie potrzeby można przywrócić oryginalny początkowy dysk RAM.

Początkowy dysk RAM jest przechowywany w pliku na komputerze. Przed zaktualizowaniem początkowego dysku RAM po raz pierwszy narzędzie Universal Restore zapisuje jego kopię w tym samym katalogu. Nazwą kopii jest nazwa pliku z sufiksem **_acronis_backup.img**. Ta kopia nie zostaje zastąpiona, gdy narzędzie Universal Restore jest uruchamiane więcej niż raz (na przykład po dodaniu brakujących sterowników).

Aby przywrócić oryginalny początkowy dysk RAM, wykonaj dowolną z następujących czynności:

- Zmień odpowiednio nazwę kopii. Wywołaj na przykład polecenie podobne do następującego:

```
mv initrd-2.6.16.60-0.21-default_acronis_backup.img
initrd-2.6.16.60-0.21-default
```

- Określ kopię w wierszu **initrd** konfiguracji programu startowego GRUB.

Copyright © Acronis International GmbH, 2002-2017

6.4 Odzyskiwanie plików

6.4.1 Odzyskiwanie plików przy użyciu interfejsu internetowego

1. Wybierz komputer, który pierwotnie zawierał dane do odzyskania.
2. Kliknij **Odzyskiwanie**.
3. Wybierz punkt odzyskiwania. Uwaga, punkty odzyskiwania są filtrowane na podstawie lokalizacji.

   Jeśli został wybrany komputer fizyczny lub komputer w trybie offline, punkty odzyskiwania nie są wyświetlane. Wybierz punkt odzyskiwania na karcie Kopie zapasowe (s. 92) lub skorzystaj z innych metod odzyskiwania:

   - Pobierz pliki z chmury (s. 83)
   - Użyj nośnika startowego (s. 84)
4. Kliknij **Odzyskaj** > **Pliki/foldery**.
5. Przejdź do potrzebnego folderu lub skorzystaj z funkcji wyszukiwania, aby uzyskać listę potrzebnych plików i folderów.

   Można użyć jednego lub kilku symboli wieloznacznych (* i ?). Aby uzyskać więcej informacji na temat stosowania symboli wieloznacznych, zobacz sekcję „Filtry plików” (s. 60).
6. Wybierz pliki, które chcesz odzyskać.
7. Jeśli chcesz zapisać pliki w pliku .zip, kliknij **Pobierz**, wybierz lokalizację, w której mają zostać zapisane dane, i kliknij **Zapisz**. W przeciwnym razie pomiń ten krok.
8. Kliknij **Odzyskaj**.

   W polu **Odzyskaj do** pojawi się jeden z następujących obiektów:

   - Komputer pierwotnie zawierający pliki, które chcesz odzyskać (jeśli znajduje się na nim agent lub maszyna wirtualna ESXi).
   - Komputer z zainstalowanym agentem dla Hyper-V (jeśli pliki pochodzą z maszyny wirtualnej Hyper-V). Plików z maszyny wirtualnej Hyper-V nie można odzyskać na pierwotną maszynę.

   Jest to komputer docelowy operacji odzyskiwania. W razie potrzeby można wybrać inny komputer.
9. [Tylko w przypadku odzyskiwania na maszynę wirtualną ESXi] Podaj poświadczenia użytkownika systemu-gościa. Użytkownik ten musi należeć do grupy **Administratorzy** w systemie Windows lub być użytkownikiem root w systemie Linux.
10. W polu **Ścieżka** wybierz miejsce docelowe odzyskiwania. Możesz wybrać jedną z następujących opcji:

    - Pierwotna lokalizacja (w przypadku odzyskiwania na pierwotny komputer)
    - Folder lokalny na komputerze docelowym
    - Folder sieciowy dostępny z komputera docelowego
11. Kliknij **Rozpocznij odzyskiwanie**.
12. Wybierz jedną z następujących opcji zastępowania plików:

    - **Zastąp istniejące pliki**
    - **Zastąp istniejący plik, jeśli jest starszy**
    - **Nie zastępuj istniejących plików**

Postęp odzyskiwania jest widoczny na karcie **Działania**.

Copyright © Acronis International GmbH, 2002-2017

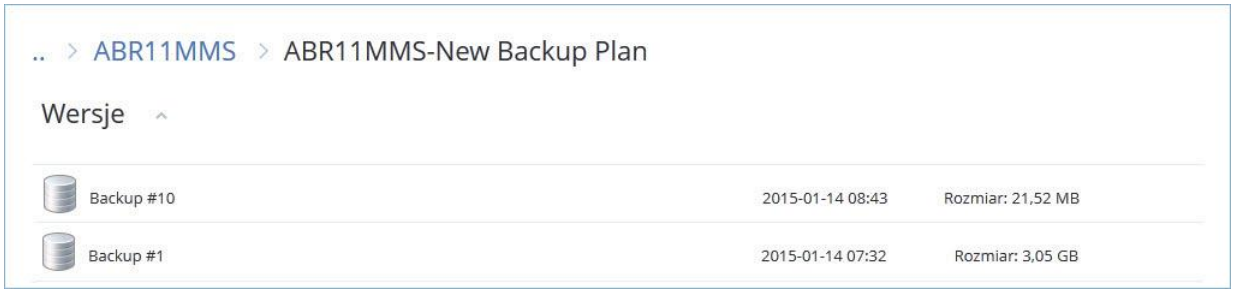
6.4.2 Pobieranie plików z chmury

Można przeglądać chmurę, wyświetlać zawartość kopii zapasowych i pobierać potrzebne pliki.

Ograniczenie: nie można przeglądać kopii zapasowych stanu systemu, baz danych SQL ani baz danych programu Exchange.

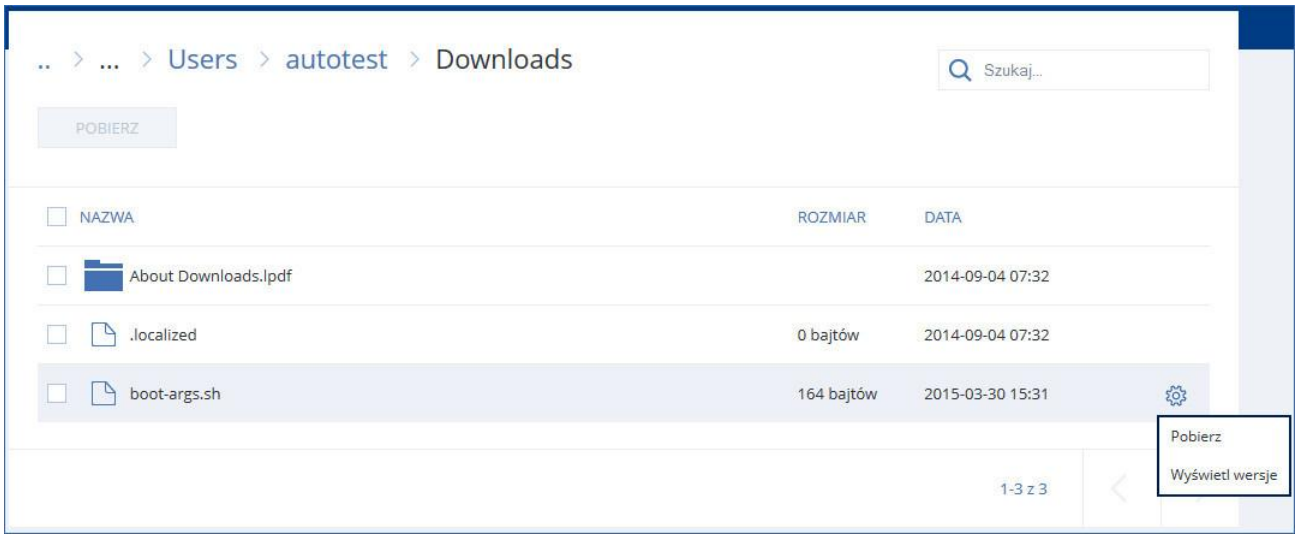
Aby pobrać pliki z chmury

1. Wybierz komputer, którego kopia zapasowa została utworzona.
2. Kliknij **Odzyskaj** > **Więcej metod odzyskiwania** > **Pobierz pliki**.
3. Wprowadź poświadczenia konta, do którego jest przypisany komputer uwzględniony w kopii zapasowej.
4. [W przypadku przeglądania kopii zapasowych na poziomie dysku] W obszarze **Wersje** kliknij kopię zapasową, z której chcesz odzyskać pliki.



[W przypadku przeglądania kopii zapasowych na poziomie plików] W następnym kroku możesz wybrać datę i godzinę kopii zapasowej, korzystając z ikony koła zębatego widocznej z prawej strony wybranego pliku. Domyślnie pliki są odzyskiwane z ostatniej kopii zapasowej.

5. Przejdź do potrzebnego folderu lub skorzystaj z funkcji wyszukiwania, aby uzyskać listę potrzebnych plików i folderów.



6. Zaznacz pola wyboru odpowiadające elementom, które chcesz odzyskać, a następnie kliknij **Pobierz**.

   Jeśli zaznaczysz jeden plik, zostanie on pobrany w jego zwykłej postaci. W przeciwnym razie wybrane dane zostaną zarchiwizowane w pliku ZIP.

7. Wybierz lokalizację, w której chcesz zapisać dane, a następnie kliknij **Zapisz**.

Copyright © Acronis International GmbH, 2002-2017

6.4.3 Odzyskiwanie plików przy użyciu nośnika startowego

Informacje na temat tworzenia nośnika startowego można znaleźć w sekcji „Tworzenie nośnika startowego” (s. 73).

Aby odzyskać pliki przy użyciu nośnika startowego

1. Uruchom komputer docelowy, korzystając z nośnika startowego.
2. Kliknij **Zarządzaj tym komputerem lokalnie** lub kliknij **Ratunkowy nośnik startowy** dwa razy, w zależności od typu używanego nośnika.
3. Jeśli w danej sieci jest włączony serwer proxy, kliknij **Narzędzia** > **Serwer proxy**, a następnie określ nazwę hosta / adres IP oraz port serwera proxy. W przeciwnym razie pomiń ten krok.
4. Na ekranie powitalnym kliknij **Odzyskaj**.
5. Kliknij **Wybierz dane**, a następnie kliknij **Przeglądaj**.
6. Określ lokalizację kopii zapasowej:
   - Aby odzyskać z chmury, wybierz **Chmura**. Wprowadź poświadczenia konta, do którego jest przypisany komputer uwzględniony w kopii zapasowej.
   - Aby odzyskać z folderu lokalnego lub sieciowego, przejdź do niego w obszarze **Foldery lokalne** lub **Foldery sieciowe**.

   Kliknij **OK**, aby zatwierdzić wybór.
7. Wybierz kopię zapasową, z której chcesz odzyskać dane. Jeśli pojawi się monit, wpisz hasło kopii zapasowej.
8. W polu **Zawartość kopii zapasowej** wybierz **Foldery/pliki**.
9. Wybierz dane, które chcesz odzyskać. Kliknij **OK**, aby zatwierdzić wybór.
10. W obszarze **Lokalizacja odzyskiwania** określ folder. Opcjonalnie możesz zablokować zastępowanie nowszych wersji plików lub wykluczyć niektóre pliki z odzyskiwania.
11. [Opcjonalnie] Kliknij **Opcje odzyskiwania**, aby określić dodatkowe ustawienia.
12. Kliknij **OK**, aby rozpocząć odzyskiwanie.

6.4.4 Wyodrębnianie plików z lokalnych kopii zapasowych

Można przeglądać zawartość kopii zapasowych i wyodrębniać potrzebne pliki.

Wymagania

- Ta funkcja jest dostępna tylko w przypadku korzystania z Eksploratora plików w systemie Windows.
- Na komputerze używanym do przeglądania kopii zapasowej musi być zainstalowany agent kopii zapasowych.
- System plików w kopii zapasowej musi być jednym z następujących: FAT16, FAT23, NTFS, ReFS, Ext2, Ext3, Ext4, XFS lub HFS+.
- Kopia zapasowa musi być przechowywana w folderze lokalnym, udziale sieciowym (SMB/CIFS) lub strefie Secure Zone.

Aby wyodrębnić pliki z kopii zapasowej

1. W Eksploratorze plików przejdź do lokalizacji kopii zapasowej.
2. Kliknij dwukrotnie plik kopii zapasowej. Nazwy plików mają następującą strukturę:

   `<nazwa komputera> - <identyfikator GUID planu tworzenia kopii zapasowych>`
3. Jeśli kopia zapasowa jest zaszyfrowana, wprowadź hasło szyfrowania. W przeciwnym razie pomiń ten krok.

Copyright © Acronis International GmbH, 2002-2017

W Eksploratorze plików zostaną wyświetlone punkty odzyskiwania.

4. Kliknij dwukrotnie odpowiedni punkt odzyskiwania.

   W Eksploratorze plików zostaną wyświetlone dane z kopii zapasowej.

5. Przejdź do odpowiedniego folderu.
6. Skopiuj potrzebne pliki do dowolnego folderu w systemie plików.

6.5 Odzyskiwanie stanu systemu

1. Wybierz komputer, którego stan systemu chcesz odzyskać.
2. Kliknij **Odzyskiwanie**.
3. Wybierz punkt odzyskiwania stanu systemu. Uwaga, punkty odzyskiwania są filtrowane na podstawie lokalizacji.
4. Kliknij **Odzyskaj stan systemu**.
5. Potwierdź, że chcesz zastąpić stan systemu jego wersją z kopii zapasowej.

Postęp odzyskiwania jest widoczny na karcie **Działania**.

6.6 Odzyskiwanie konfiguracji ESXi

Do odzyskania konfiguracji ESXi potrzebny jest nośnik startowy oparty na systemie Linux. Informacje na temat tworzenia nośnika startowego można znaleźć w sekcji „Tworzenie nośnika startowego” (s. 73).

Jeśli odzyskujesz konfigurację ESXi na host inny niż pierwotny, a pierwotny host ESXi jest nadal podłączony do serwera vCenter, rozłącz ten host i usuń go z serwera vCenter, aby uniknąć niespodziewanych problemów podczas odzyskiwania. Jeśli chcesz zachować pierwotny host razem z odzyskanym, możesz go dodać ponownie po zakończeniu operacji odzyskiwania.

Maszyny wirtualne działające na hoście nie są uwzględniane w kopii zapasowej konfiguracji ESXi. Można jednak osobno tworzyć ich kopie zapasowe i osobno je odzyskiwać.

Aby odzyskać konfigurację ESXi

1. Uruchom komputer docelowy, korzystając z nośnika startowego.
2. Kliknij **Zarządzaj tym komputerem lokalnie**.
3. Jeśli kopia zapasowa znajduje się w chmurze, do której dostęp uzyskuje się przez serwer proxy, kliknij **Narzędzia** > **Server proxy** i określ nazwę hosta / adres IP oraz port serwera proxy. W przeciwnym razie pomiń ten krok.
4. Na ekranie powitalnym kliknij **Odzyskaj**.
5. Kliknij **Wybierz dane**, a następnie kliknij **Przeglądaj**.
6. Określ lokalizację kopii zapasowej:
   - Przejdź do folderu w obszarze **Foldery lokalne** lub **Foldery sieciowe**.

   Kliknij **OK**, aby zatwierdzić wybór.
7. W polu **Pokaż** wybierz **Konfiguracje ESXi**.
8. Wybierz kopię zapasową, z której chcesz odzyskać dane. Jeśli pojawi się monit, wpisz hasło kopii zapasowej.
9. Kliknij **OK**.
10. W polu **Dyski, które mają zostać wykorzystane na potrzeby nowych magazynów danych** zrób tak:

Copyright © Acronis International GmbH, 2002-2017

- W obszarze **Odzyskaj ESXi na** wybierz dysk, na który zostanie odzyskana konfiguracja hosta. W przypadku odzyskiwania konfiguracji na pierwotny host domyślnie zostaje wybrany dysk oryginalny.
- [Opcjonalnie] W obszarze **Użyj dla nowych magazynów danych** wybierz dyski, na których zostaną utworzone nowe magazyny danych. Zrób to z rozwagą, ponieważ wszystkie dane zapisane na wybranych dyskach zostaną utracone. Jeśli chcesz zachować maszyny wirtualne w istniejących już magazynach danych, nie wybieraj żadnego dysku.

11. Jeśli nie wybierzesz dysków na potrzeby nowych magazynów danych, w polu **Jak utworzyć nowe magazyny danych** wybierz metodę utworzenia magazynów danych: **Utwórz jeden magazyn danych na dysk** lub **Utwórz jeden magazyn danych na wszystkich wybranych dyskach twardych**.
12. [Opcjonalnie] W polu **Mapowanie sieci** zmień wynik automatycznego mapowania przełączników wirtualnych dostępnych w kopii zapasowej na fizyczne karty sieciowe.
13. [Opcjonalnie] Kliknij **Opcje odzyskiwania**, aby określić dodatkowe ustawienia.
14. Kliknij **OK**, aby rozpocząć odzyskiwanie.

6.7 Opcje odzyskiwania

Aby zmodyfikować opcje odzyskiwania, kliknij **Opcje odzyskiwania** podczas konfigurowania odzyskiwania.

Dostępne opcje odzyskiwania

Zakres dostępnych opcji odzyskiwania zależy od następujących czynników:

- Środowisko działania agenta wykonującego operację odzyskiwania (Windows, Linux, OS X lub nośnik startowy)
- Typ odzyskiwanych danych (dyski, pliki, maszyny wirtualne, dane aplikacji)

W poniższej tabeli zestawiono dostępność opcji odzyskiwania.

	Dyski			**Pliki**				**Maszyny wirtualne**	**SQL oraz Exchange**
	Windows	Linux	Nośnik startowy	Windows	Linux	OS X	Nośnik startowy	ESXi i Hyper-V	Windows
Sprawdzanie poprawności kopii zapasowej (s. 87)	+	+	+	+	+	+	+	+	+
Data i godzina plików (s. 87)	-	-	-	+	+	+	+	-	-
Obsługa błędów (s. 88)	+	+	+	+	+	+	+	+	+
Wykluczenia plików (s. 88)	-	-	-	+	+	+	+	-	-
Zabezpieczenia na poziomie plików (s. 88)	-	-	-	+	+	+	+	-	-
Flashback (s. 89)	-	-	-	-	-	-	-	+	-

Copyright © Acronis International GmbH, 2002-2017

	Dyski			Pliki				Maszyny wirtualne	SQL oraz Exchange
	Windows	Linux	Nośnik startowy	Windows	Linux	OS X	Nośnik startowy	ESXi i Hyper-V	Windows
Odzyskiwanie pełnej ścieżki (s. 89)	-	-	-	+	+	+	+	-	-
Punkty zamontowania (s. 89)	-	-	-	+	-	-	-	-	-
Wydajność (s. 89)	+	+	-	+	+	+	-	+	+
Polecenia poprzedzające/następujące (s. 90)	+	+	-	+	+	+	-	+	+
Zmiana identyfikatorów SID (s. 91)	+	-	-	-	-	-	-	-	-
Zarządzanie zasilaniem maszyn wirtualnych (s. 91)	-	-	-	-	-	-	-	+	-
Dziennik zdarzeń systemu Windows (s. 92)	+	-	-	+	-	-	-	Tylko Hyper-V	+

6.7.1 Sprawdzanie poprawności kopii zapasowej

Opcja określa, czy przed odzyskaniem danych z kopii zapasowej należy sprawdzić jej poprawność. Dzięki temu można się upewnić, że kopia zapasowa nie jest uszkodzona.

Ustawienie wstępne: **Wyłączone**.

Sprawdzanie poprawności polega na obliczeniu sumy kontrolnej każdego bloku danych zapisanego w kopii zapasowej. Jedynym wyjątkiem jest sprawdzanie poprawności kopii zapasowych na poziomie plików znajdujących się w chmurze. Sprawdzenie poprawności tych kopii zapasowych polega na sprawdzeniu spójności zapisanych w nich metainformacji.

Sprawdzanie poprawności jest czasochłonne — nawet w przypadku przyrostowych lub różnicowych kopii zapasowych, które mają niewielkie rozmiary. Dzieje się tak, ponieważ w trakcie tej operacji sprawdzana jest poprawność nie tylko danych zawartych fizycznie w kopii zapasowej, ale również wszystkich danych, które można odzyskać po wybraniu tej kopii. Wymaga to uzyskania dostępu do utworzonych wcześniej kopii zapasowych.

6.7.2 Data i godzina plików

Ta opcja jest dostępna tylko podczas odzyskiwania plików.

Copyright © Acronis International GmbH, 2002-2017

Opcja określa, czy data i godzina plików mają być odzyskiwane z kopii zapasowej, czy też do plików ma być przypisywana bieżąca data i godzina.

W przypadku włączenia tej opcji plikom będą przypisywane bieżąca data i godzina.

Ustawienie wstępne: **Włączona**.

6.7.3 Obsługa błędów

Umożliwiają one określenie sposobu obsługi błędów, które mogą wystąpić podczas odzyskiwania.

W razie błędu spróbuj ponownie

Ustawienie wstępne: **Włączone. Liczba prób: 30. Odstęp między próbami: 30 s.**

Po wystąpieniu błędu, który można naprawić, program próbuje ponownie wykonać operację zakończoną niepowodzeniem. Można ustawić odstęp między 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.

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.

6.7.4 Wykluczenia plików

Ta opcja jest dostępna tylko podczas odzyskiwania plików.

Opcja określa, które pliki i foldery należy pominąć w procesie odzyskiwania, a tym samym wykluczyć z listy odzyskiwanych elementów.

Uwaga *Wykluczenia mają wyższy priorytet niż wybór elementów danych do odzyskania. Jeśli na przykład wybierzesz do odzyskania plik MójPlik.tmp i wykluczysz wszystkie pliki .tmp, plik MójPlik.tmp nie zostanie odzyskany.*

6.7.5 Zabezpieczenia na poziomie plików

Ta opcja jest dostępna tylko w przypadku odzyskiwania z kopii zapasowej na poziomie plików zawierającej pliki systemu Windows.

Opcja określa, czy razem z plikami mają być odzyskiwane uprawnienia do plików pochodzące z systemu NTFS.

Ustawienie wstępne: **Włączona**.

Jeśli uprawnienia NTFS zostały zachowane podczas tworzenia kopii zapasowej (s. 62), można określić, czy należy je odzyskać, czy pliki powinny odziedziczyć uprawnienia NTFS z folderu, do którego są odzyskiwane.

Copyright © Acronis International GmbH, 2002-2017

6.7.6 Flashback

Ta opcja jest dostępna w przypadku odzyskiwania na maszynę wirtualną wykonywanego przez agenta dla VMware lub agenta dla Hyper-V.

Technologia Flashback przyspiesza odzyskiwanie maszyn wirtualnych. Jeśli ta opcja jest włączona, odzyskiwane są tylko różnice między kopią zapasową a lokalizacją docelową. Dane są porównywane na poziomie bloków.

Ustawienie wstępne: **Włączona**.

6.7.7 Odzyskiwanie pełnej ścieżki

Ta opcja jest dostępna tylko w przypadku odzyskiwania danych z kopii zapasowej na poziomie plików.

Jeśli ta opcja jest włączona, w lokalizacji docelowej zostanie odtworzona pełna ścieżka pliku.

Ustawienie wstępne: **Wyłączone**.

6.7.8 Punkty zamontowania

Ta opcja jest dostępna tylko w systemie Windows w przypadku odzyskiwania danych z kopii zapasowej na poziomie pliku.

Włącz tę opcję, aby odzyskać pliki i foldery przechowywane na zamontowanych woluminach, których kopie zapasowe zostały wykonane przy włączonej opcji Punkty zamontowania (s. 63).

Ustawienie wstępne: **Wyłączone**.

Ta opcja jest dostępna tylko wtedy, gdy wybrany folder do odzyskania znajduje się wyżej w hierarchii folderów niż punkt zamontowania. Jeśli wskażesz do operacji odzyskiwania foldery znajdujące się wewnątrz punktu zamontowania lub sam punkt zamontowania, wybrane elementy zostaną odzyskane bez względu na wartość opcji **Punkty zamontowania**.

Uwaga *Należy pamiętać, że jeśli wolumin nie jest zamontowany w momencie odzyskiwania, dane zostaną odzyskane bezpośrednio do folderu, który był określony jak punkt zamontowania podczas tworzenia kopii zapasowej.*

6.7.9 Wydajność

Ta opcja umożliwia określenie priorytetu procesu odzyskiwania w systemie operacyjnym.

Dostępne są następujące ustawienia: **Niski**, **Normalny**, **Wysoki**.

Ustawienie wstępne: **Normalny**.

Priorytet procesu działającego w systemie określa ilość mocy obliczeniowej procesora i zasobów systemowych przydzielonych do tego procesu. Obniżenie priorytetu odzyskiwania zwolni więcej zasobów na potrzeby pozostałych aplikacji. Podwyższenie priorytetu odzyskiwania może przyspieszyć proces odzyskiwania przez żądanie przydzielenia przez system operacyjny większej ilości zasobów aplikacji odzyskującej. Jednak efekt takiej operacji będzie zależał od całkowitego wykorzystania mocy obliczeniowej procesora oraz innych czynników, takich jak szybkość operacji we/wy na dysku czy natężenie ruchu w sieci.

Copyright © Acronis International GmbH, 2002-2017

6.7.10 Polecenia poprzedzające/następujące

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 z logicznym systemem plików, błędów fizycznych lub uszkodzonych sektorów przed rozpoczęciem odzyskiwania lub po jego zakończeniu.

Program nie obsługuje poleceń interaktywnych, czyli wymagających wpisania tekstu przez użytkownika (na przykład „pause").

Polecenia po zakończeniu odzyskiwania nie zostaną wykonane, jeśli proces odzyskiwania uruchomi ponownie komputer.

6.7.10.1 Polecenie poprzedzające odzyskiwanie

Aby określić polecenie/plik wsadowy do wykonania przed rozpoczęciem procesu odzyskiwania

1. Włącz przełącznik **Wykonaj polecenie przed odzyskaniem**.
2. W polu **Polecenie** wpisz polecenie lub wyszukaj plik wsadowy. Program nie obsługuje poleceń interaktywnych, czyli wymagających wpisania tekstu przez użytkownika (na przykład „pause").
3. W polu **Katalog roboczy** określ ścieżkę katalogu, w którym zostanie wykonane polecenie lub plik wsadowy.
4. W polu **Argumenty** w razie potrzeby określ argumenty wykonywania polecenia.
5. W zależności od wyniku, który chcesz uzyskać, wybierz odpowiednie opcje opisane w poniższej tabeli.
6. Kliknij **Gotowe**.

Pole wyboru	**Wybór**			
Zakończ odzyskiwanie niepowodzeniem, jeśli wykonanie polecenia się nie powiedzie*	Wybrane	Niewybrane	Wybrane	Niewybrane
Nie przeprowadzaj odzyskiwania przed zakończeniem wykonywania polecenia	Wybrane	Wybrane	Niewybrane	Niewybrane
Wynik				
	Ustawienie wstępne Przeprowadź odzyskiwanie dopiero po pomyślnym wykonaniu polecenia. Zakończ odzyskiwanie niepowodzeniem, jeśli wykonanie polecenia się nie powiodło.	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 uznaje się za niewykonane, jeśli jego kod zakończenia jest różny od zera.

Copyright © Acronis International GmbH, 2002-2017

6.7.10.2 Polecenie po zakończeniu odzyskiwania

Aby określić polecenie/plik wykonywalny, które mają zostać wykonane po zakończeniu odzyskiwania

1. Włącz przełącznik **Wykonaj polecenie po odzyskaniu**.
2. W polu **Polecenie** wpisz polecenie lub wyszukaj plik wsadowy.
3. W polu **Katalog roboczy** określ ścieżkę katalogu, w którym zostanie wykonane polecenie lub plik wsadowy.
4. W polu **Argumenty** w razie potrzeby określ argumenty wykonywania polecenia.
5. Jeśli pomyślne wykonanie polecenia ma znaczenie krytyczne, zaznacz pole wyboru **Zakończ odzyskiwanie niepowodzeniem, jeśli wykonanie polecenia się nie powiedzie**. Polecenie uznaje się za niewykonane, jeśli jego kod zakończenia jest różny od zera. W takim przypadku zostanie ustawiony status odzyskiwania **Błąd**.

   Jeśli to pole wyboru nie jest zaznaczone, wynik wykonania polecenia nie wpływa na powodzenie lub niepowodzenie operacji odzyskiwania. Wynik wykonania polecenia można sprawdzić, przeglądając kartę **Działania**.
6. Kliknij **Gotowe**.

Uwaga *Polecenia po zakończeniu odzyskiwania nie zostaną wykonane, jeśli proces odzyskiwania uruchomi ponownie komputer.*

6.7.11 Zmiana identyfikatorów SID

Ta opcja jest dostępna w przypadku odzyskiwania systemu Windows 8.1/Windows Server 2012 R2 lub starszego.

Ta opcja nie jest dostępna w przypadku odzyskiwania na maszynę wirtualną wykonywanego przez agenta dla VMware lub agenta dla Hyper-V.

Ustawienie wstępne: **Wyłączone**.

Oprogramowanie może wygenerować unikatowy identyfikator zabezpieczeń (SID komputera) dla odzyskiwanego systemu operacyjnego. Ta opcja jest potrzebna tylko do zapewnienia działania oprogramowania innych firm, które korzysta z identyfikatora SID komputera.

Oficjalnie firma Microsoft nie zapewnia obsługi zmiany identyfikatora SID we wdrażanym lub odzyskiwanym systemie. Dlatego tej opcji używa się na własne ryzyko.

6.7.12 Zarządzanie zasilaniem maszyn wirtualnych

Te opcje są dostępne w przypadku odzyskiwania na maszynę wirtualną wykonywanego przez agenta dla VMware lub agenta dla Hyper-V.

Przed uruchomieniem odzyskiwania wyłącz docelowe maszyny wirtualne

Ustawienie wstępne: **Włączona**.

Odzyskanie na istniejącą maszynę wirtualną nie jest możliwe, jeśli jest ona w trybie online, dlatego natychmiast po rozpoczęciu odzyskiwania maszyna jest automatycznie wyłączana. Użytkownicy są odłączani od maszyny, a wszelkie niezapisane dane zostaną utracone.

Jeśli wolisz ręcznie wyłączać maszyny wirtualne przed rozpoczęciem odzyskiwania, wyczyść pole wyboru tej opcji.

Copyright © Acronis International GmbH, 2002-2017

Włącz docelową maszynę wirtualną po zakończeniu odzyskiwania

Ustawienie wstępne: **Wyłączone**.

Po odzyskaniu maszyny z kopii zapasowej na inną maszynę, w sieci może się pojawić replika istniejącej maszyny. Na wszelki wypadek po zastosowaniu niezbędnych środków ostrożności ręcznie włącz odzyskaną maszynę wirtualną.

6.7.13 Dziennik zdarzeń systemu Windows

Ta opcja jest dostępna tylko w systemach operacyjnych Windows.

Opcja umożliwia określenie, czy agenty muszą rejestrować zdarzenia operacji odzyskiwania w dzienniku zdarzeń aplikacji systemu Windows (aby wyświetlić ten dziennik, uruchom plik eventvwr.exe lub wybierz **Panel sterowania** > **Narzędzia administracyjne** > **Podgląd zdarzeń**). Zdarzenia, które mają być rejestrowane, można filtrować.

Ustawienie wstępne: **Wyłączone**.

7 Operacje dotyczące kopii zapasowych

7.1 Karta Kopie zapasowe

Na karcie **Kopie zapasowe** są wyświetlane kopie zapasowe wszystkich komputerów kiedykolwiek zarejestrowanych na serwerze zarządzania. Dotyczy to także komputerów będących w trybie offline oraz komputerów, które nie są już zarejestrowane.

Kopie zapasowe przechowywane w lokalizacji współużytkowanej (takiej jak udział SMB lub NFS) są widoczne dla wszystkich użytkowników mających uprawnienia do odczytu w danej lokalizacji.

W chmurze użytkownicy mają dostęp tylko do własnych kopii zapasowych. W przypadku wdrożenia chmurowego administrator może przeglądać kopie zapasowe na każdym koncie należącym do tej samej grupy i jej grup podrzędnych. Konto to jest wybierane pośrednio w polu **Komputer używany do przeglądania**. Na karcie **Kopie zapasowe** są wyświetlane kopie zapasowe wszystkich komputerów kiedykolwiek zarejestrowanych w ramach tego samego konta, na którym jest zarejestrowany dany komputer.

Lokalizacje kopii zapasowych używane w planach tworzenia kopii zapasowych są automatycznie dodawane na karcie **Kopie zapasowe**. Aby dodać folder niestandardowy (na przykład odłączane urządzenie USB) do listy lokalizacji kopii zapasowych, kliknij **Przeglądaj** i określ ścieżkę folderu.

Aby wybrać punkt odzyskiwania na karcie Kopie zapasowe

1. Na karcie **Kopie zapasowe** wybierz lokalizację, w której są przechowywane kopie zapasowe.

   W oprogramowaniu zostaną wyświetlone wszystkie kopie zapasowe z wybranej lokalizacji, które można zobaczyć z danego konta. Kopie te są zestawione w grupy. Nazwy grup są oparte na następującym szablonie:

   `<nazwa komputera> — <nazwa planu tworzenia kopii zapasowych>`
2. Wybierz grupę, z której chcesz odzyskać dane.
3. [Opcjonalnie] Kliknij **Zmień** obok pozycji **Komputer używany do przeglądania**, a następnie wybierz inny komputer. Niektóre kopie zapasowe można przeglądać tylko przy użyciu określonych agentów. Na przykład w celu przeglądania kopii zapasowych baz danych programu Microsoft SQL Server trzeba wybrać komputer z agentem dla SQL.

Copyright © Acronis International GmbH, 2002-2017

Ważne *Warto pamiętać, że* ***Komputer używany do przeglądania*** *jest domyślnym miejscem docelowym odzyskiwania z kopii zapasowej komputera fizycznego. Po wybraniu punktu odzyskiwania i kliknięciu* ***Odzyskaj*** *dokładnie sprawdź ustawienie* ***Komputer docelowy****, aby się upewnić, że został wybrany komputer, na który chcesz odzyskać dane. Aby zmienić miejsce docelowe odzyskiwania, określ w polu* ***Komputer używany do przeglądania*** *inny komputer.*

4. Kliknij **Pokaż kopie zapasowe**.
5. Wybierz punkt odzyskiwania.

7.2 Montowanie woluminów z kopii zapasowej

Montowanie woluminów z kopii zapasowej na poziomie dysku pozwala na dostęp do woluminów w taki sam sposób jak do dysków fizycznych. Woluminy są montowane w trybie tylko do odczytu.

Wymagania

- Ta funkcja jest dostępna tylko w przypadku korzystania z Eksploratora plików w systemie Windows.
- Na komputerze wykonującym operację montowania musi być zainstalowany agent dla systemu Windows.
- Wersja systemu Windows działającego na komputerze musi obsługiwać system plików z kopii zapasowej.
- Kopia zapasowa musi być przechowywana w folderze lokalnym, udziale sieciowym (SMB/CIFS) lub strefie Secure Zone.

Aby zamontować wolumin z kopii zapasowej

1. W Eksploratorze plików przejdź do lokalizacji kopii zapasowej.
2. Kliknij dwukrotnie plik kopii zapasowej. Nazwy plików mają następującą strukturę:

   `<nazwa komputera> - <identyfikator GUID planu tworzenia kopii zapasowych>`
3. Jeśli kopia zapasowa jest zaszyfrowana, wprowadź hasło szyfrowania. W przeciwnym razie pomiń ten krok.

   W Eksploratorze plików zostaną wyświetlone punkty odzyskiwania.
4. Kliknij dwukrotnie odpowiedni punkt odzyskiwania.

   W Eksploratorze plików zostaną wyświetlone woluminy z kopii zapasowej.

Wskazówka *Kliknij dwukrotnie wolumin, aby przejrzeć jego zawartość. Pliki i foldery z kopii zapasowej możesz skopiować do dowolnego folderu w systemie plików.*

5. Kliknij prawym przyciskiem myszy montowany wolumin, a następnie kliknij **Zamontuj w trybie tylko do odczytu**.
6. Jeśli kopia zapasowa jest przechowywana w udziale sieciowym, podaj poświadczenia dostępu. W przeciwnym razie pomiń ten krok.

   Oprogramowanie zamontuje wybrany wolumin. Do tego woluminu zostanie przypisana pierwsza wolna litera.

Aby odmontować wolumin

1. W Eksploratorze plików przejdź do obszaru **Komputer** (**Ten komputer PC** w systemie Windows 8.1 lub nowszym).
2. Kliknij prawym przyciskiem myszy zamontowany wolumin.
3. Kliknij **Odmontuj**.

   Oprogramowanie odmontuje wybrany wolumin.

Copyright © Acronis International GmbH, 2002-2017

7.3 Usuwanie kopii zapasowych

Aby usunąć kopie zapasowe komputera będącego w trybie online i dostępnego w konsoli kopii zapasowych

1. Na karcie **Wszystkie urządzenia** zaznacz komputer, którego kopie zapasowe chcesz usunąć.
2. Kliknij **Odzyskiwanie**.
3. Wybierz lokalizację, z której chcesz usunąć kopie zapasowe.
4. Wykonaj jedną z następujących czynności:
   - Aby usunąć jedną kopię zapasową, zaznacz ją, a następnie kliknij ikonę kosza.
   - Aby usunąć wszystkie kopie zapasowe z wybranej lokalizacji, kliknij **Usuń wszystko**.
5. Potwierdź decyzję.

Aby usunąć kopie zapasowe dowolnego komputera

1. Na karcie **Kopie zapasowe** wybierz lokalizację, z której chcesz usunąć kopie zapasowe.

   W oprogramowaniu zostaną wyświetlone wszystkie kopie zapasowe z wybranej lokalizacji, które można zobaczyć z danego konta. Kopie te są zestawione w grupy. Nazwy grup są oparte na następującym szablonie:

   `<nazwa komputera> - <nazwa planu tworzenia kopii zapasowych>`
2. Wybierz grupę.
3. Wykonaj jedną z następujących czynności:
   - Aby usunąć jedną kopię zapasową, kliknij **Pokaż kopie zapasowe**, zaznacz kopię zapasową przeznaczoną do usunięcia, a następnie kliknij ikonę kosza.
   - Aby usunąć wybraną grupę, kliknij **Usuń**.
4. Potwierdź decyzję.

8 Operacje dotyczące planów tworzenia kopii zapasowych

Aby edytować plan tworzenia kopii zapasowych

1. Jeśli chcesz edytować plan tworzenia kopii zapasowych dla wszystkich komputerów, do których jest on stosowany, wybierz jeden z tych komputerów. W innym przypadku wybierz komputery, dla których chcesz edytować plan tworzenia kopii zapasowych.
2. Kliknij **Kopia zapasowa**.
3. Wybierz plan tworzenia kopii zapasowych, który chcesz edytować.
4. Kliknij ikonę koła zębatego widoczną obok nazwy planu tworzenia kopii zapasowych, a następnie kliknij **Edytuj**.
5. Aby zmodyfikować parametry planu, kliknij odpowiednią sekcję w panelu planu tworzenia kopii zapasowych.
6. Kliknij **Zapisz zmiany**.
7. Aby zmienić plan tworzenia kopii zapasowych dla wszystkich komputerów, do których jest on stosowany, kliknij **Zastosuj zmiany do tego planu tworzenia kopii zapasowych**. W innym przypadku kliknij **Utwórz nowy plan tworzenia kopii zapasowych tylko dla wybranych urządzeń**.

Aby odwołać plan tworzenia kopii zapasowych na komputerach

1. Wybierz komputery, których plan tworzenia kopii zapasowych chcesz odwołać.
2. Kliknij **Kopia zapasowa**.

Copyright © Acronis International GmbH, 2002-2017

3. Jeśli do tych komputerów jest stosowanych kilka planów tworzenia kopii zapasowych, wybierz plan, który chcesz odwołać.
4. Kliknij ikonę koła zębatego widoczną obok nazwy danego planu tworzenia kopii zapasowych, a następnie kliknij **Odwołaj**.

Aby usunąć plan tworzenia kopii zapasowych

1. Wybierz dowolny komputer, do którego jest stosowany plan tworzenia kopii zapasowych przeznaczony do usunięcia.
2. Kliknij **Kopia zapasowa**.
3. Jeśli do tego komputera jest stosowanych kilka planów tworzenia kopii zapasowych, wybierz plan, który chcesz usunąć.
4. Kliknij ikonę koła zębatego widoczną obok nazwy planu tworzenia kopii zapasowych, a następnie kliknij **Usuń**.

   W wyniku tego plan tworzenia kopii zapasowych zostanie odwołany ze wszystkich komputerów i całkowicie usunięty z interfejsu internetowego.

9 Generator nośnika startowego

Generator nośnika startowego to specjalne narzędzie do tworzenia nośnika startowego. Jest ono dostępne tylko w ramach wdrożeń lokalnych.

Generator nośnika startowego jest instalowany domyślnie podczas instalacji serwera zarządzania. Generator nośnika można zainstalować osobno na każdym komputerze z systemem Windows lub Linux. Obsługiwane są te same systemy operacyjne co w przypadku odpowiednich agentów.

Dlaczego warto korzystać z generatora nośnika?

Nośnika startowego dostępnego do pobrania w konsoli kopii zapasowych można używać tylko w celu odzyskiwania. Nośnik ten jest oparty na jądrze systemu Linux. W odróżnieniu od środowiska Windows PE takie jądro nie umożliwia wprowadzania do systemu niestandardowych sterowników w locie.

- Generator nośnika pozwala na utworzenie dostosowanego nośnika startowego opartego na systemie Linux lub środowisku WinPE i obsługującego tworzenie kopii zapasowych.
- Oprócz utworzenia nośnika fizycznego lub jego obrazu ISO możliwe jest przesłanie nośnika do usług Windows Deployment Services (WDS) i skorzystanie z funkcji uruchamiania przez sieć.
- I wreszcie można zapisać nośnik bezpośrednio na dysku flash — bez użycia narzędzi innych firm.

Wersja 32- czy 64-bitowa?

Generator nośnika startowego można zainstalować przy użyciu programu instalacyjnego w wersji zarówno 32-, jak i 64-bitowej. Bitowość nośnika jest zgodna z bitowością programu instalacyjnego. Można jednak utworzyć nośnik oparty na 32-bitowym środowisku WinPE przy użyciu 64-bitowego generatora nośnika, o ile zostanie pobrana 32-bitowa wtyczka.

Warto pamiętać, że w większości przypadków do uruchomienia komputera korzystającego z interfejsu Unified Extensible Firmware Interface (UEFI) potrzebny jest nośnik 64-bitowy.

9.1 Nośnik startowy oparty na systemie Linux

Aby utworzyć nośnik startowy oparty na systemie Linux

1. Uruchom Generator nośnika startowego.

Copyright © Acronis International GmbH, 2002-2017

2. Określ klucz licencyjny. Licencja nie zostanie przypisana ani nie zostanie zmienione jej przypisanie. Decyduje ona o tym, które funkcje mają zostać włączone dla tworzonego nośnika. Bez kluczy licencyjnych można utworzyć nośnik służący tylko do odzyskiwania.
3. Wybierz **Typ nośnika startowego: Domyślny (oparty na systemie Linux)**.

   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 z obsługą woluminów w stylu systemu Windows wyświetla woluminy na przykład jako C: i D:. Zapewnia dostęp do woluminów dynamicznych (LDM).
4. [Opcjonalnie] Określ parametry jądra systemu Linux. W przypadku wielu parametrów należy je rozdzielić spacjami.

   Aby na przykład mieć możliwość wyboru trybu wyświetlania agenta startowego przy każdym uruchomieniu nośnika, wpisz: **vga=ask**

   Aby zapoznać się z listą parametrów, zobacz Parametry jądra (s. 97).
5. Wybierz komponenty, które zostaną umieszczone na nośniku: agenta startowego i/lub narzędzie Universal Restore.

   Używając nośnika z agentem startowym, można na dowolnym komputerze kompatybilnym ze standardem PC wykonywać operacje tworzenia kopii zapasowych i odzyskiwania oraz zarządzania dyskami, włącznie z odzyskiwaniem systemu po awarii.

   Narzędzie Universal Restore umożliwia uruchomienie systemu operacyjnego odzyskanego na komputer o innej konfiguracji sprzętowej lub maszynę wirtualną w razie problemów z jego uruchomieniem. Narzędzie to znajduje i instaluje sterowniki urządzeń, które mają zasadnicze znaczenie z perspektywy uruchamiania systemu operacyjnego, takie jak sterowniki kontrolerów pamięci masowej, płyty głównej czy chipsetu.
6. [Opcjonalnie] Określ limit czasu menu startowego oraz komponent uruchamiany automatycznie w przypadku przekroczenia tego limitu.

   Jeśli ta opcja nie zostanie skonfigurowana, program ładujący czeka, aż użytkownik podejmie decyzję o uruchomieniu systemu operacyjnego (jeśli jest dostępny) lub komponentu.

   Jeśli ustawisz na przykład **10 s** dla agenta startowego, agent zostanie uruchomiony po upływie 10 s od wyświetlenia menu. Umożliwia to wykonywanie na miejscu nienadzorowanej operacji w przypadku uruchamiania z serwera WDS/RIS.
7. [Opcjonalnie] Określ ustawienia zdalnego logowania: nazwę użytkownika i hasło do podania w ciągu polecenia, jeśli narzędzie **acrocmd** działa na innym komputerze. Jeśli te pola pozostaną puste, polecenie nie musi obejmować poświadczeń.
8. [Opcjonalnie] Określ ustawienia sieciowe (s. 98): ustawienia TCP/IP, które mają zostać przypisane do kart sieciowych komputera.
9. [Opcjonalnie] Określ port sieciowy (s. 99): port TCP, na którym agent startowy nasłuchuje połączeń przychodzących.
10. [Opcjonalnie] Jeśli w sieci jest włączony serwer proxy, określ jego nazwę hosta / adres IP oraz port.
11. Wybierz typ tworzonego nośnika. Użytkownik może:

    - Utworzyć płytę CD, DVD lub inny nośnik startowy, na przykład wymienny dysk flash USB, jeśli system BIOS sprzętu pozwala na uruchamianie z takiego nośnika.
    - Wygenerować obraz ISO do późniejszego nagrania na czystej płycie lub podłączenia do maszyny wirtualnej.
    - Przesłać wybrane komponenty na serwer WDS/RIS.

Copyright © Acronis International GmbH, 2002-2017

12. [Opcjonalnie] Dodaj sterowniki przeznaczone do użycia przez narzędzie Universal Restore (s. 99) w systemie Windows. To okno jest wyświetlane, jeśli na nośniku umieszczono narzędzie Universal Restore i wybrano nośnik inny niż serwer WDS/RIS.
13. Jeśli pojawi się stosowny monit, określ nazwę hosta / adres IP oraz poświadczenia serwera WDS/RIS lub ścieżkę do pliku ISO nośnika.
14. Na ekranie podsumowania sprawdź ustawienia i kliknij **Kontynuuj**.

9.1.1 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 określić, 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

Copyright © Acronis International GmbH, 2002-2017

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.

9.1.2 Ustawienia sieciowe

Podczas tworzenia nośnika startowego dostępna jest opcja wstępnego skonfigurowania połączeń sieciowych, których będzie używać agent startowy. Można skonfigurować następujące parametry:

- Adres IP
- Maska podsieci
- Brama
- Serwer DNS
- Serwer WINS

Po uruchomieniu agenta startowego na komputerze konfiguracja jest stosowana do karty sieciowej tego komputera. Jeśli ustawienia nie zostały wstępnie skonfigurowane, agent używa automatycznej konfiguracji DHCP. Po uruchomieniu agenta startowego na komputerze ustawienia sieciowe można też skonfigurować ręcznie.

Copyright © Acronis International GmbH, 2002-2017

Wstępne konfigurowanie wielu połączeń sieciowych

Można wstępnie skonfigurować ustawienia TCP/IP dla nawet dziesięciu kart sieciowych. Aby mieć pewność, że do każdej karty sieciowej zostaną przypisane właściwe ustawienia, należy utworzyć nośnik na serwerze, do którego nośnik został dostosowany. Gdy zaznaczysz istniejącą kartę sieciową w oknie kreatora, jej ustawienia zostają wybrane do zapisania na nośniku. Na nośniku jest też zapisywany adres MAC każdej dostępnej karty sieciowej.

Ustawienia, z wyjątkiem adresu MAC, można zmienić. W razie potrzeby można też skonfigurować ustawienia nieistniejącej karty NIC.

Gdy agent startowy uruchomi się na serwerze, pobiera listę dostępnych kart sieciowych. Lista ta jest uporządkowana według gniazd zajmowanych przez karty: na początku są wymienione karty znajdujące się najbliżej procesora.

Agent startowy przypisuje odpowiednie ustawienia każdej znanej karcie sieciowej, rozpoznając poszczególne karty na podstawie ich adresów MAC. Po skonfigurowaniu kart sieciowych o znanych adresach MAC do pozostałych kart są przypisywane ustawienia określone dla kart nieistniejących, począwszy od znajdującej się najwyżej nieprzypisanej karty.

Nośnik startowy można dostosować pod kątem każdego komputera — nie tylko tego, na którym nośnik został utworzony. W tym celu należy skonfigurować karty sieciowe zgodnie z kolejnością ich gniazd w komputerze: karta NIC1 zajmuje gniazdo znajdujące się najbliżej procesora, karta NIC2 kolejne gniazdo itd. Gdy agent startowy uruchomi się na komputerze, nie znajdzie żadnej karty sieciowej ze znanym adresem MAC, w związku z czym skonfiguruje karty w takiej samej kolejności.

Przykład

Agent startowy może używać jednej z kart sieciowych do komunikacji z konsolą zarządzania za pośrednictwem sieci produkcyjnej. Połączenie to może zostać skonfigurowane automatycznie. Duże ilości danych związanych z odzyskiwaniem można przesłać za pośrednictwem drugiej karty sieciowej, uwzględnionej w odrębnej sieci tworzenia kopii zapasowych przy użyciu statycznych ustawień TCP/IP.

9.1.3 Port sieciowy

Podczas tworzenia nośnika startowego można wstępnie skonfigurować port sieciowy, na którym agent startowy będzie nasłuchiwać połączenia przychodzącego z narzędzia **acrocmd**. Dostępne są następujące opcje:

- port domyślny,
- aktualnie używany port,
- nowy port (należy wprowadzić jego numer).

Jeśli port nie zostanie wstępnie skonfigurowany, agent użyje portu 9876.

9.1.4 Sterowniki dla narzędzia Universal Restore

Podczas tworzenia nośnika startowego można dodać do niego sterowniki dla systemu Windows. Za pomocą tych nośników narzędzie Universal Restore będzie uruchamiać system Windows, który migrowano do innej konfiguracji sprzętowej.

W narzędziu Universal Restore możliwe będzie skonfigurowanie:

- wyszukiwania na nośniku sterowników najlepiej dopasowanych do docelowej konfiguracji sprzętowej,

Copyright © Acronis International GmbH, 2002-2017

- pobierania z nośnika jawnie określonych sterowników pamięci masowej. Jest to konieczne, gdy docelowa konfiguracja sprzętowa obejmuje określony kontroler pamięci masowej dla dysku twardego (taki jak adapter SCSI, RAID lub Fibre Channel).

Sterowniki zostaną umieszczone w widocznym folderze Drivers na nośniku startowym. Sterowniki nie są ładowane do pamięci RAM docelowegokomputera, dlatego nośnik musi być stale włożony lub podłączony za pośrednictwem narzędzia Universal Restore.

Dodawanie sterowników do nośnika startowego jest możliwe podczas tworzenia nośnika wymiennego lub jego obrazu ISO, a także podczas tworzenia nośnika odłączanego, takiego jak dysk flash. Sterowników nie można przesyłać na serwer WDS/RIS.

Sterowniki można dodawać do listy tylko w grupach, dodając pliki INF lub foldery zawierające takie pliki. Wybór poszczególnych sterowników z plików INF nie jest możliwy, ale generator nośnika wyświetla zawartość pliku w celach informacyjnych.

Aby dodać sterowniki:

1. Kliknij **Dodaj** i odszukaj plik INF lub folder zawierający pliki INF.
2. Wybierz plik INF lub folder.
3. Kliknij **OK**.

Sterowniki można usuwać z listy tylko w grupach, usuwając pliki INF.

Aby usunąć sterowniki:

1. Wybierz plik INF.
2. Kliknij **Usuń**.

9.2 Nośnik startowy oparty na środowisku WinPE

Generator nośnika startowego oferuje trzy metody integracji programu Acronis Backup ze środowiskiem WinPE:

- Tworzenie 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.).

Generator nośnika startowego obsługuje dystrybucje środowiska WinPE oparte na następujących jądrach:

- Windows Vista (PE 2.0)
- Windows Vista z dodatkiem SP1 i Windows Server 2008 (PE 2.1)
- Windows 7 (PE 3.0) z uzupełnieniem dla systemu Windows 7 SP1 (PE 3.1) lub bez niego
- Windows 8 (PE 4,0)
- Windows 8.1 (PE 5.0)
- Windows 10 (PE dla systemu Windows 10)

Generator nośnika startowego obsługuje 32- oraz 64-bitowe dystrybucje środowiska WinPE. 32-bitowa dystrybucja środowiska WinPE może działać także na sprzęcie 64-bitowym. Jednak do uruchomienia komputera korzystającego z interfejsu Unified Extensible Firmware Interface (UEFI) potrzebna jest dystrybucja 64-bitowa.

Do działania obrazów PE opartych na środowisku WinPE 4 lub nowszym wymagany jest przynajmniej 1 GB pamięci RAM.

Copyright © Acronis International GmbH, 2002-2017

9.2.1 Przygotowanie: Środowisko WinPE 2.x lub 3.x

Aby można było tworzyć lub modyfikować obrazy środowiska PE 2.x lub 3.x, zainstaluj Generator nośnika startowego na komputerze, na którym jest zainstalowany Zestaw zautomatyzowanej instalacji systemu Windows (AIK). Jeśli na komputerze nie jest zainstalowany zestaw AIK, wykonaj opisane poniżej czynności przygotowawcze.

Aby przygotować komputer z zestawem AIK

1. Pobierz i zainstaluj Zestaw zautomatyzowanej instalacji systemu Windows.

   Zestaw zautomatyzowanej instalacji systemu Windows (AIK) dla systemu Windows Vista (PE 2.0):

   http://www.microsoft.com/Downloads/details.aspx?familyid=C7D4BC6D-15F3-4284-9123-679830D629F2&displaylang=pl

   Zestaw zautomatyzowanej instalacji systemu Windows (AIK) dla systemu Windows Vista z dodatkiem SP1 i systemu 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 (AIK) dla systemu Windows 7 (PE 3.0):

   http://www.microsoft.com/downloads/details.aspx?familyid=696DD665-9F76-4177-A811-39C26D3B3B34&displaylang=pl

   Uzupełnienie zestawu zautomatyzowanej instalacji (AIK) dla systemu Windows 7 z dodatkiem SP1 (PE 3.1):

   http://www.microsoft.com/pl-pl/download/details.aspx?id=5188

   Informacje o wymaganiach systemowych instalacji można znaleźć, korzystając z powyższych łączy.
2. [Opcjonalnie] Nagraj zestaw AIK na płytę DVD lub skopiuj go na dysk flash.
3. Zainstaluj środowisko Microsoft .NET Framework z tego zestawu (NETFXx86 lub NETFXx64 w zależności od konfiguracji sprzętowej komputera).
4. Zainstaluj analizator Microsoft Core XML (MSXML) 5.0 lub 6.0 z tego zestawu.
5. Zainstaluj zestaw Windows AIK z tego zestawu.
6. Zainstaluj Generator nośnika startowego na tym samym komputerze.

Zaleca się zapoznanie z dokumentacją pomocy dostarczoną z zestawem Windows AIK. Aby uzyskać dostęp do dokumentacji, wybierz **Microsoft Windows AIK -> Dokumentacja** z menu startowego.

9.2.2 Przygotowanie: środowisko WinPE 4.0 lub nowsze

Aby umożliwić tworzenie i modyfikowanie obrazów środowiska PE 4 lub nowszego, zainstaluj Generator nośnika startowego na komputerze z zainstalowanym Zestawem do oceny i wdrażania systemu Windows (ADK). Jeśli na komputerze nie jest zainstalowany zestaw ADK, wykonaj opisane poniżej czynności przygotowawcze.

Aby przygotować komputer z zestawem ADK

1. Pobierz program instalacyjny Zestawu do oceny i wdrażania systemu Windows.

   Zestaw do oceny i wdrażania systemu Windows (ADK) dla systemu Windows 8 (PE 4,0): http://www.microsoft.com/en-us/download/details.aspx?id=30652.

   Zestaw do oceny i wdrażania systemu Windows (ADK) dla systemu Windows 8.1 (PE 5.0): http://www.microsoft.com/en-US/download/details.aspx?id=39982.

Copyright © Acronis International GmbH, 2002-2017

Zestaw do oceny i wdrażania systemu Windows (ADK) dla systemu Windows 10 (PE dla systemu Windows 10):
https://msdn.microsoft.com/pl-pl/windows/hardware/dn913721%28v=vs.8.5%29.aspx.

Informacje o wymaganiach systemowych instalacji można znaleźć, korzystając z powyższych łączy.

2. Zainstaluj na komputerze Zestaw do oceny i wdrażania systemu Windows.
3. Zainstaluj Generator nośnika startowego na tym samym komputerze.

9.2.3 Dodawanie wtyczki Acronis Plug-in do środowiska WinPE

Aby dodać wtyczkę Acronis Plug-in do środowiska WinPE:

1. Uruchom Generator nośnika startowego.
2. Określ klucze licencyjne. Klucze licencyjne nie zostaną przypisane ani nie zostanie zmienione ich przypisanie. Decydują one o tym, które funkcje mają zostać włączone dla tworzonego nośnika. Bez kluczy licencyjnych można utworzyć nośnik służący tylko do odzyskiwania.
3. Wybierz **Typ nośnika startowego: Windows PE** lub **Typ nośnika startowego: Windows PE (64-bitowy)**. Nośnik 64-bitowy jest potrzebny do uruchomienia komputera korzystającego z interfejsu Unified Extensible Firmware Interface (UEFI).

   W przypadku wybrania opcji **Typ nośnika startowego: Windows PE** najpierw wykonaj następujące czynności:

   - Kliknij **Pobierz wtyczkę dla środowiska WinPE (32-bitową)**.
   - Zapisz wtyczkę w folderze **%PROGRAM_FILES%\Acronis\BootableComponents\WinPE32**.

   Jeśli planujesz odzyskać system operacyjny na komputerze o innej konfiguracji sprzętowej lub na maszynie wirtualnej i chcesz zapewnić możliwość uruchamiania systemu, zaznacz pole wyboru **Uwzględnij narzędzie Universal Restore**.
4. Wybierz **Utwórz WinPE automatycznie**.

   Oprogramowanie uruchamia odpowiedni skrypt i przechodzi do kolejnego okna.
5. Określ, czy należy włączyć, czy wyłączyć połączenie zdalne z komputerem uruchamianym z nośnika. W przypadku włączenia tej funkcji wprowadź nazwę użytkownika i hasło do podania w wierszu polecenia, jeśli narzędzie **acrocmd** działa na innym komputerze. Jeśli pozostawisz te pola puste, połączenie zdalne będzie wyłączone.
6. Określ ustawienia sieciowe (s. 98) kart sieciowych komputera lub wybierz automatyczną konfigurację DHCP.
7. [Opcjonalnie] Określ sterowniki Windows, które chcesz dodać do środowiska Windows PE.

   Po uruchomieniu komputera w środowisku Windows PE sterowniki ułatwiają dostęp do urządzenia, na którym znajduje się kopia zapasowa. Dodaj sterowniki 32-bitowe, jeśli jest używana 32-bitowa dystrybucja środowiska WinPE, lub sterowniki 64-bitowe w przypadku 64-bitowej dystrybucji środowiska WinPE.

   Wskazanie dodanych sterowników będzie także możliwe podczas konfigurowania narzędzia Universal Restore dla systemu Windows. Na potrzeby korzystania z narzędzia Universal Restore należy dodać sterowniki 32- lub 64-bitowe, zależnie od tego, czy operacja odzyskiwania ma dotyczyć systemu Windows w wersji 32- czy 64-bitowej.

   Aby dodać sterowniki:

   - Kliknij **Dodaj** i określ ścieżkę do niezbędnego pliku *.inf dla odpowiadającego mu kontrolera SCSI, RAID, SATA, adaptera sieciowego, napędu taśmowego lub innego urządzenia.
   - Powtórz tę procedurę dla każdego sterownika, który chcesz dołączyć do wynikowego nośnika środowiska WinPE.

Copyright © Acronis International GmbH, 2002-2017

8. Wybierz, czy chcesz utworzyć obraz ISO czy obraz WIM, lub prześlij nośnik na serwer (WDS lub RIS).
9. Określ pełną ścieżkę do wynikowego pliku obrazu, włącznie z nazwą pliku, lub określ serwer i podaj nazwę użytkownika oraz hasło umożliwiające do niego dostęp.
10. Na ekranie podsumowania sprawdź ustawienia i kliknij **Kontynuuj**.
11. 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 agent uruchamia się automatycznie.

Aby utworzyć obraz środowiska PE (plik ISO) z wynikowego pliku WIM:

- Zastąp domyślny plik boot.wim w folderze środowiska Windows PE nowo utworzonym plikiem WIM. W powyższym przykładzie wpisz:

  ```
  copy c:\AcronisMedia.wim c:\winpe_x86\ISO\sources\boot.wim
  ```

- Użyj narzędzia **Oscdimg**. W powyższym przykładzie wpisz:

  ```
  oscdimg -n -bc:\winpe_x86\etfsboot.com c:\winpe_x86\ISO
  c:\winpe_x86\winpe_x86.iso
  ```

  Nie kopiuj i nie wklejaj tego przykładu. Wpisz polecenie ręcznie, ponieważ w przeciwnym razie jego wykonanie się nie powiedzie.

Aby uzyskać więcej informacji na temat dostosowywania środowiska Windows PE 2.x i 3.x, zobacz Windows Preinstallation Environment User's Guide (Podręcznik użytkownika środowiska preinstalacyjnego systemu Windows) (Winpe.chm). Informacje na temat dostosowywania środowiska Windows PE 4.0 lub nowszego są dostępne w bibliotece Microsoft TechNet.

10 Ochrona urządzeń mobilnych

Do tworzenia kopii zapasowych danych przechowywanych na urządzeniach mobilnych i ich odzyskiwania należy używać aplikacji do tworzenia kopii zapasowych.

Obsługiwane urządzenia mobilne

- Smartfony i tablety z systemem Android w wersji 4.1 lub nowszej.
- iPhone'y, iPady i iPody z systemem iOS w wersji 8 lub nowszej.

Elementy, które można uwzględnić w kopii zapasowej

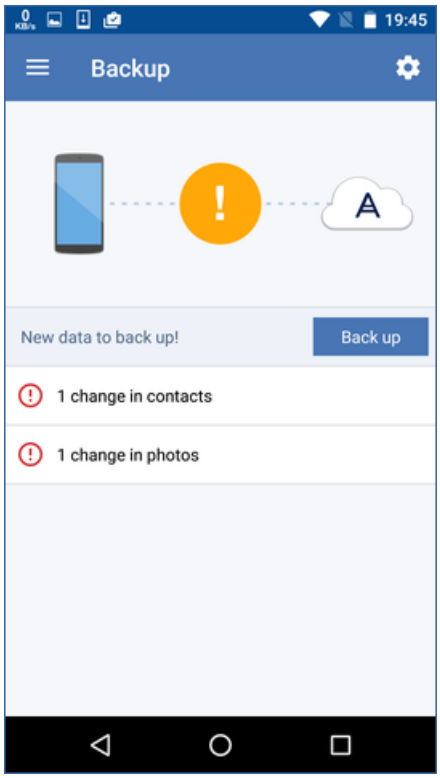
- Kontakty
- Zdjęcia
- Wideo
- Kalendarze
- SMS-y (tylko na urządzeniach z systemem Android)
- Przypomnienia (tylko na urządzeniach z systemem iOS)

Co trzeba wiedzieć

- Kopie zapasowe danych można tworzyć tylko w chmurze.

Copyright © Acronis International GmbH, 2002-2017

- Przy każdym otwarciu aplikacji wyświetlane jest podsumowanie zmian w danych i można ręcznie rozpocząć tworzenie kopii zapasowej.



- Funkcja **Ciągła kopia zapasowa** jest domyślnie włączona. W tym trybie aplikacja do tworzenia kopii zapasowych co 6 godzin sprawdza, czy dane uległy zmianie, i w razie wykrycia zmian automatycznie uruchamia operację tworzenia kopii zapasowej. Funkcję ciągłej kopii zapasowej można wyłączyć. Można też zmienić ustawienia aplikacji na **Tylko podczas ładowania**.
- Dane z kopii zapasowej są dostępne na każdym urządzeniu mobilnym zarejestrowanym na danym koncie. Dzięki temu można łatwiej przenosić dane ze starego urządzenia mobilnego na nowe. Kontakty i zdjęcia z urządzenia z systemem Android można odzyskać na urządzenie z systemem iOS — i na odwrót. Zdjęcie, film lub kontakt można też pobrać na komputer za pomocą konsoli kopii zapasowych.
- Uwzględnione w kopii zapasowej dane z urządzenia mobilnego zarejestrowanego na koncie są widoczne tylko na tym koncie. Nikt inny nie może wyświetlić ani odzyskać Twoich danych.
- W aplikacji do tworzenia kopii zapasowych można odzyskać dane tylko z najnowszej kopii zapasowej. Jeśli potrzebujesz danych ze starszej kopii zapasowej, skorzystaj z konsoli kopii zapasowych na tablecie lub komputerze.
- W przypadku kopii zapasowych urządzeń mobilnych reguły przechowywania nie mają zastosowania.
- Jeśli podczas tworzenia kopii zapasowej w urządzeniu znajduje się karta SD, w kopii zapasowej zostaną uwzględnione również dane z tej karty. Dane te zostaną odzyskane na kartę SD, jeśli podczas odzyskiwania będzie ona dostępna w urządzeniu. W przeciwnym razie zostaną odzyskane do magazynu wewnętrznego.
- Bez względu na to, czy pierwotne dane były przechowywane w magazynie wewnętrznym urządzenia, czy na karcie SIM, odzyskane dane zostaną umieszczone w magazynie wewnętrznym.

Szczegółowe instrukcje

Aby uzyskać aplikację do tworzenia kopii zapasowych

1. Na urządzeniu mobilnym otwórz przeglądarkę i przejdź do strony https://backup.acronis.com/.

Copyright © Acronis International GmbH, 2002-2017

2. Zaloguj się przy użyciu konta Acronis.
3. Kliknij **Wszystkie urządzenia** > **Dodaj**.
4. W obszarze **Urządzenia mobilne** wybierz typ urządzenia.

   W zależności od typu urządzenia, nastąpi przekierowanie do sklepu App Store lub sklepu Google Play Store.
5. [Tylko w przypadku urządzeń z systemem iOS] Kliknij **Pobierz**.
6. Kliknij **Zainstaluj**, aby zainstalować aplikację do tworzenia kopii zapasowych.

Aby rozpocząć tworzenie kopii zapasowych danych urządzenia z systemem iOS

1. Otwórz aplikację do tworzenia kopii zapasowych.
2. Zaloguj się przy użyciu konta Acronis.
3. Wybierz kategorie danych, które chcesz uwzględnić w kopii zapasowej. Domyślnie wybrane są wszystkie kategorie.
4. Stuknij **Utwórz kopię zapasową**.
5. Zezwól aplikacji na dostęp do Twoich danych osobistych. Jeśli odmówisz dostępu do niektórych kategorii danych, nie będą one uwzględniane w kopiach zapasowych.

Rozpocznie się operacja tworzenia kopii zapasowych.

Aby rozpocząć tworzenie kopii zapasowych danych urządzenia z systemem Android

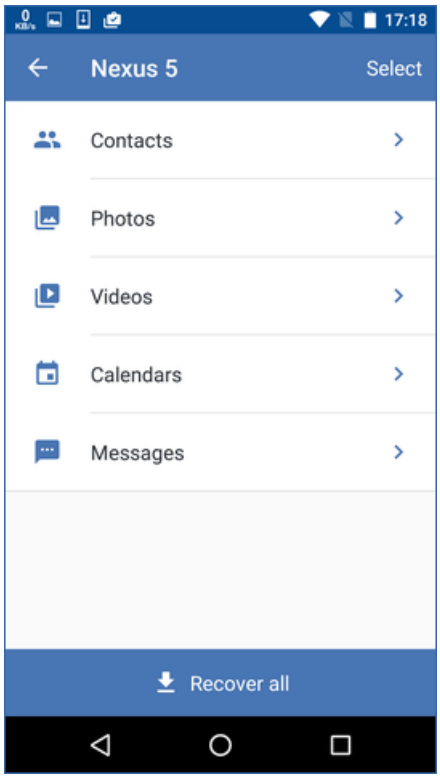
1. Otwórz aplikację do tworzenia kopii zapasowych.
2. Zaloguj się przy użyciu konta Acronis.
3. [W przypadku systemu Android w wersji 6.0 lub nowszej] Zezwól aplikacji na dostęp do Twoich danych osobistych. Jeśli odmówisz dostępu do niektórych kategorii danych, nie będą one uwzględniane w kopiach zapasowych.
4. [Opcjonalnie] Określ kategorie danych, których nie chcesz uwzględniać w kopiach zapasowych. W tym celu stuknij ikonę koła zębatego, stuknij suwaki kategorii danych, które chcesz wykluczyć z kopii zapasowych, a następnie stuknij strzałkę Wstecz.
5. Stuknij **Utwórz kopię zapasową**.

Aby odzyskać dane na urządzenie mobilne

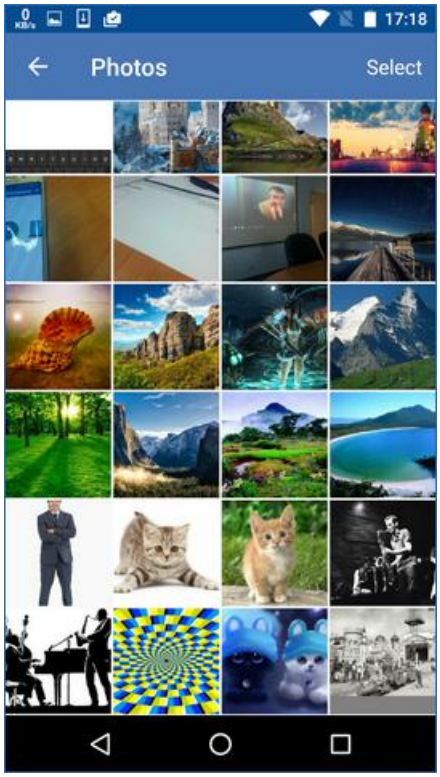
1. Otwórz aplikację do tworzenia kopii zapasowych.
2. Przesuń palce w prawo i stuknij **Dostęp i odzyskiwanie**.
3. Stuknij nazwę urządzenia.
4. Wykonaj jedną z następujących czynności:
   - Aby odzyskać wszystkie dane z kopii zapasowej, stuknij **Odzyskaj wszystko**. Nie trzeba wykonywać żadnych innych czynności.
   - Aby odzyskać tylko wybrane kategorie danych, stuknij **Wybierz**, a następnie stuknij pola wyboru wymaganych kategorii danych. Stuknij **Odzyskaj**. Nie trzeba wykonywać żadnych innych czynności.

Copyright © Acronis International GmbH, 2002-2017

- Aby odzyskać tylko wybrane elementy danych należące do tej samej kategorii danych, stuknij odpowiednią kategorię danych. Przejdź do kolejnych działań.



5. Wykonaj jedną z następujących czynności:
   - Aby odzyskać jeden element danych, stuknij go.
   - Aby odzyskać kilka elementów danych, stuknij **Wybierz**, a następnie stuknij pola wyboru wymaganych elementów danych.

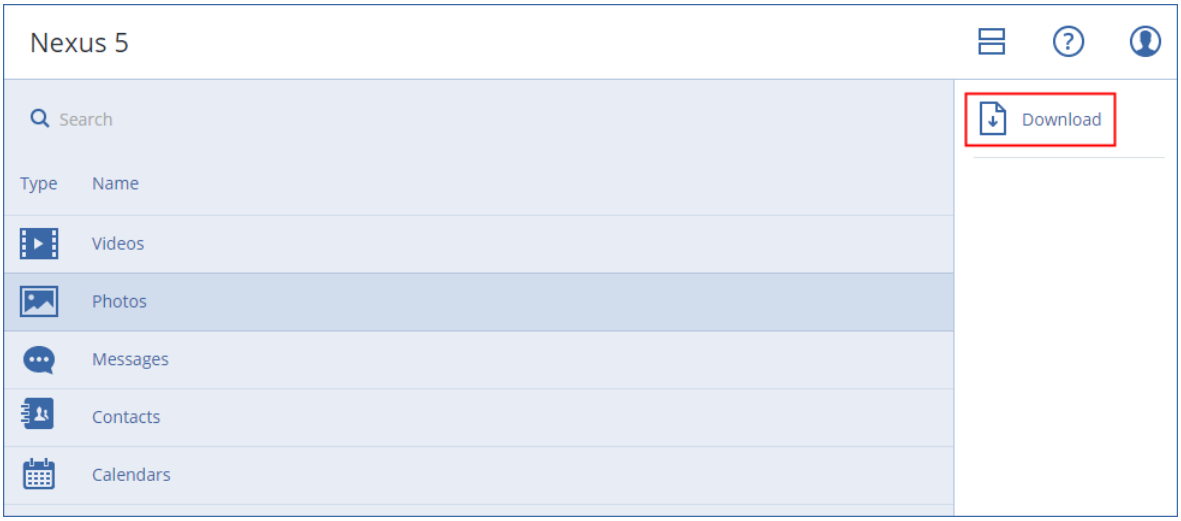


6. Stuknij **Odzyskaj**.

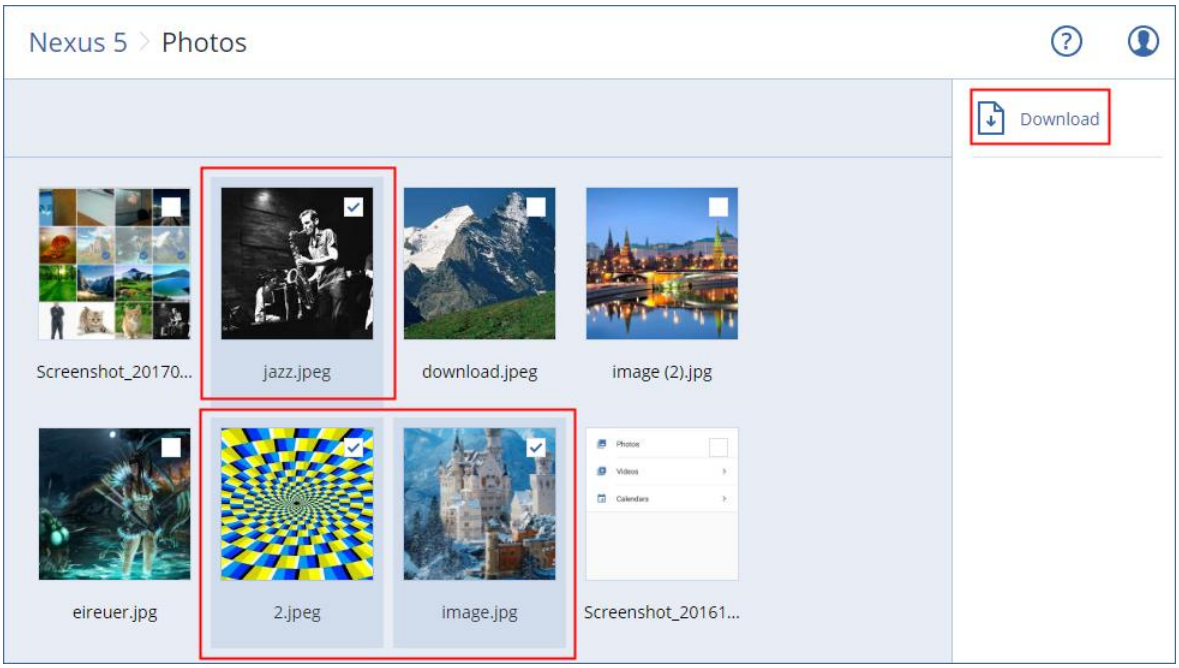
Copyright © Acronis International GmbH, 2002-2017

Aby uzyskać dostęp do danych za pomocą konsoli kopii zapasowych

1. Na komputerze otwórz przeglądarkę i przejdź do strony https://backup.acronis.com/.
2. Zaloguj się przy użyciu konta Acronis.
3. W obszarze **Wszystkie urządzenia** zaznacz nazwę odpowiedniego urządzenia mobilnego i kliknij **Odzyskaj**.
4. Wybierz punkt odzyskiwania.
5. Wykonaj dowolne z następujących czynności:
   - Aby pobrać wszystkie zdjęcia, filmy lub kontakty, wybierz odpowiednią kategorię danych. Kliknij **Pobierz**.



   - Aby pobrać wybrane zdjęcia, filmy lub kontakty, kliknij nazwę odpowiedniej kategorii danych, a następnie zaznacz pola wyboru wymaganych elementów danych. Kliknij **Pobierz**.



   - Aby wyświetlić podgląd wiadomości tekstowej, zdjęcia lub kontaktu, kliknij nazwę odpowiedniej kategorii danych, a następnie kliknij wymagany element danych.

Więcej informacji można znaleźć na stronie https://docs.acronis.com/mobile-backup. Pomoc jest dostępna również w aplikacji do tworzenia kopii zapasowych (naciśnij **Ustawienia** > **Pomoc** w menu aplikacji).

Copyright © Acronis International GmbH, 2002-2017

11 Chronienie aplikacji

Chronienie programów Microsoft SQL Server i Microsoft Exchange Server

Dostępne są dwie metody ochrony tych aplikacji:

- **Kopia zapasowa bazy danych**

  Jest to kopia zapasowa na poziomie plików uwzględniająca bazy danych oraz powiązane z nimi metadane. Bazy danych można odzyskać do działających aplikacji lub jako pliki.

- **Kopia zapasowa uwzględniająca aplikacje**

  Jest to kopia zapasowa na poziomie dysku, która gromadzi również metadane aplikacji. Metadane te umożliwiają przeglądanie i odzyskiwanie danych aplikacji bez odzyskiwania całego dysku lub woluminu. Możliwe jest również odzyskanie całego dysku lub woluminu. Dzięki temu można używać jednego rozwiązania i jednego planu tworzenia kopii zapasowych do odzyskiwania po awarii oraz ochrony danych.

Ochrona programu Microsoft SharePoint

Farma programu Microsoft SharePoint zawiera serwery frontonu z działającymi usługami programu SharePoint, serwery baz danych z uruchomionym programem Microsoft SQL Server oraz (opcjonalnie) serwery aplikacji, które odciążają serwery typu frontonu, przejmując część usług programu SharePoint. Niektóre serwery frontonu i serwery aplikacji mogą być identyczne.

Aby chronić całą farmę programu SharePoint:

- Utwórz kopię zapasową wszystkich serwerów baz danych przy użyciu kopii zapasowej uwzględniającej aplikacje.
- Utwórz kopię zapasową wszystkich unikatowych serwerów frontonu i serwerów aplikacji przy użyciu zwykłej kopii zapasowej na poziomie dysku.

Kopie zapasowe wszystkich serwerów powinny zostać utworzone na podstawie tego samego harmonogramu.

Aby chronić tylko zawartość, można osobno utworzyć kopie zapasowe baz danych zawartości.

Chronienie kontrolera domeny

Komputer z uruchomionymi usługami domenowymi Active Directory można chronić przy użyciu kopii zapasowej uwzględniającej aplikacje. Jeśli domena zawiera więcej niż jeden kontroler domeny i jeden z nich zostanie odzyskany, wykonywane jest przywracanie nieautorytatywne i po odzyskaniu nie nastąpi wycofanie numeru USN.

Odzyskiwanie aplikacji

W poniższej tabeli zestawiono dostępne metody odzyskiwania aplikacji.

	Z kopii zapasowej baz danych	Z kopii zapasowej uwzględniającej aplikacje	Z kopii zapasowej dysku
Microsoft SQL Server	Bazy danych do działającej instancji serwera SQL (s. 113) Bazy danych jako pliki (s. 113)	Cały komputer (s. 74) Bazy danych do działającej instancji serwera SQL (s. 113) Bazy danych jako pliki (s. 113)	Cały komputer (s. 74)

Copyright © Acronis International GmbH, 2002-2017

Microsoft Exchange Server	Bazy danych do działającego programu Exchange (s. 116) Bazy danych jako pliki (s. 116) Odzyskiwanie granularne do działającego programu Exchange (s. 117)	Cały komputer (s. 74) Bazy danych do działającego programu Exchange (s. 116) Bazy danych jako pliki (s. 116) Odzyskiwanie granularne do działającego programu Exchange (s. 117)	Cały komputer (s. 74)
Serwery baz danych programu Microsoft SharePoint	Bazy danych do działającej instancji serwera SQL (s. 113) Bazy danych jako pliki (s. 113) Odzyskiwanie granularne przy użyciu programu SharePoint Explorer	Cały komputer (s. 74) Bazy danych do działającej instancji serwera SQL (s. 113) Bazy danych jako pliki (s. 113) Odzyskiwanie granularne przy użyciu programu SharePoint Explorer	Cały komputer (s. 74)
Internetowe serwery frontonu programu Microsoft SharePoint	-	-	Cały komputer (s. 74)
Usługi domenowe Active Directory	-	Cały komputer (s. 74)	-

11.1 Wymagania wstępne

Przed skonfigurowaniem kopii zapasowej aplikacji dopilnuj, aby zostały spełnione niżej wymienione wymagania.

Aby sprawdzić stan składników zapisywania usługi VSS, skorzystaj z polecenia **`vssadmin list writers`**.

Typowe wymagania

W przypadku programu Microsoft SQL Server upewnij się, że:

- Jest uruchomiona co najmniej jedna instancja programu Microsoft SQL Server.
- Są włączone usługa SQL Server Browser Service i protokół TCP/IP. Aby uzyskać informacje na temat uruchamiania usługi SQL Server Browser Service, zobacz: https://msdn.microsoft.com/pl-pl/library/ms189093.aspx. Protokół TCP/IP można włączyć, wykonując podobną procedurę.
- Jest włączony moduł zapisujący SQL dla usługi VSS.

W przypadku programu Microsoft Exchange Server upewnij się, że:

- Jest uruchomiona usługa Magazyn informacji programu Microsoft Exchange.
- Jest zainstalowane oprogramowanie Windows PowerShell. W przypadku programu Exchange 2010 lub nowszego wymagane jest oprogramowanie Windows PowerShell w wersji 2.0 lub nowszej.
- Jest zainstalowane oprogramowanie Microsoft .NET Framework.

  W przypadku programu Exchange 2007 wymagane jest oprogramowanie Windows .NET Framework w wersji 2.0 lub nowszej.

Copyright © Acronis International GmbH, 2002-2017

W przypadku programu Exchange 2010 lub nowszego wymagane jest oprogramowanie Windows .NET Framework w wersji 3.5 bądź nowszej.

- Moduł zapisujący programu Exchange dla usługi VSS jest włączony.

Na kontrolerze domeny upewnij się, że:

- Jest włączony moduł zapisujący Active Directory dla usługi VSS.

Podczas tworzenia planu tworzenia kopii zapasowych upewnij się, że:

- W przypadku komputerów fizycznych jest włączona opcja tworzenia kopii zapasowych Usługa kopiowania woluminów w tle (VSS) (s. 70).
- W przypadku maszyn wirtualnych jest włączona opcja tworzenia kopii zapasowych Usługa kopiowania woluminów w tle (VSS) dla maszyn wirtualnych (s. 72).

Dodatkowe wymagania dotyczące kopii zapasowych uwzględniających aplikacje

Podczas tworzenia planu tworzenia kopii zapasowych dopilnuj, aby dla kopii zapasowej została wybrana opcja **Cały komputer**.

Jeśli aplikacje działają na maszynach wirtualnych, których kopie zapasowe tworzy agent dla VMware, upewnij się, że:

- Maszyny wirtualne uwzględniane w kopii zapasowej spełniają wymagania wyciszenia spójnego z aplikacjami wymienione w następującym artykule bazy wiedzy VMware: https://pubs.vmware.com/vsphere-60/index.jsp?topic=%2Fcom.vmware.vddk.pg.doc%2FvddkBkupVadp.9.6.html
- Na maszynach są zainstalowane aktualne narzędzia VMware Tools.
- Na maszynach jest wyłączona usługa kontroli konta użytkownika (UAC). Jeśli nie chcesz wyłączyć usługi UAC, podczas włączania tworzenia kopii zapasowej aplikacji musisz podać poświadczenia wbudowanego administratora domeny (DOMAIN\Administrator).

11.2 Kopia zapasowa bazy danych

Przed utworzeniem kopii zapasowej baz danych dopilnuj, aby zostały spełnione wymagania wymienione w sekcji „Wymagania wstępne” (s. 109).

Wybierz bazy danych zgodnie z poniższymi instrukcjami, a następnie określ w odpowiedni sposób (s. 42) ustawienia planu tworzenia kopii zapasowych.

11.2.1 Wybieranie baz danych SQL

Kopia zapasowa bazy danych SQL zawiera pliki bazy danych (.mdf, .ndf), pliki dziennika (.ldf) i inne powiązane pliki. Kopia zapasowa tych plików jest tworzona przy użyciu usługi zapisywania programu SQL Server. Usługa ta musi być uruchomiona, gdy Usługa kopiowania woluminów w tle (VSS) zażąda utworzenia kopii zapasowej lub odzyskania.

Po każdym pomyślnym utworzeniu kopii zapasowej są obcinane dzienniki transakcji SQL. Obcinanie dzienników SQL można wyłączyć w opcjach planu tworzenia kopii zapasowych (s. 62).

Aby wybrać bazy danych SQL

1. Kliknij **Microsoft SQL**.

   Pojawią się komputery z zainstalowanym agentem dla SQL.
2. Przejdź do danych, które chcesz uwzględnić w kopii zapasowej.

Copyright © Acronis International GmbH, 2002-2017

Kliknij dwukrotnie komputer, aby wyświetlić znajdujące się na nim instancje programu SQL Server. Kliknij dwukrotnie wybraną instancję, aby wyświetlić zawarte w niej bazy danych.

3. Wybierz dane, które chcesz uwzględnić w kopii zapasowej. Możesz wybrać całe instancje lub poszczególne bazy danych.
   - W przypadku wybrania całych instancji programu SQL Server w kopii zapasowej będą uwzględniane wszystkie bieżące bazy danych oraz wszystkie bazy danych, które w przyszłości zostaną dodane do wybranych instancji.
   - W przypadku bezpośredniego wybrania baz danych w kopii zapasowej będą uwzględniane tylko wybrane bazy danych.
4. Kliknij **Kopia zapasowa**. Jeśli pojawi się monit, podaj poświadczenia umożliwiające dostęp do danych programu SQL Server. Konto musi należeć do grupy **Operatorzy kopii zapasowych** lub **Administratorzy** na danym komputerze oraz do roli **administratora systemu** w każdej instancji uwzględnianej w kopii zapasowej.

11.2.2 Wybieranie danych programu Exchange Server

Poniższa tabela zawiera zestawienie danych programu Microsoft Exchange Server, które można wybrać do uwzględnienia w kopii zapasowej, oraz minimalne prawa użytkownika wymagane w celu utworzenia kopii zapasowej tych danych.

Wersja programu Exchange	Elementy danych	Prawa użytkownika
2007	Grupy magazynów	Członkostwo w grupie z rolą **Administratorzy organizacji korzystającej z programu Exchange**
2010/2013/2016	Bazy danych	Członkostwo w grupie z rolą **Zarządzanie organizacją**.

Pełna kopia zapasowa zawiera wszystkie wybrane dane programu Exchange Server.

Przyrostowa kopia zapasowa zawiera zmienione bloki plików baz danych, pliki punktów kontrolnych oraz niewielką liczbę plików dziennika nowszych niż odpowiedni punkt kontrolny bazy danych. Ponieważ w kopii zapasowej są uwzględniane zmiany wprowadzone w plikach baz danych, nie trzeba tworzyć kopii zapasowej wszystkich wpisów dzienników transakcji utworzonych od ostatniej kopii zapasowej. Tylko dziennik nowszy niż punkt kontrolny wymaga odtworzenia po odzyskaniu. Zapewnia to szybsze odzyskiwanie i pomyślne tworzenie kopii zapasowych baz danych, nawet przy włączonym rejestrowaniu cyklicznym.

Pliki dzienników transakcji są obcinane po każdym pomyślnym utworzeniu kopii zapasowej.

Aby wybrać dane programu Exchange Server

1. Kliknij **Microsoft Exchange**.

   Pojawią się komputery z zainstalowanym agentem dla programu Exchange.
2. Przejdź do danych, które chcesz uwzględnić w kopii zapasowej.

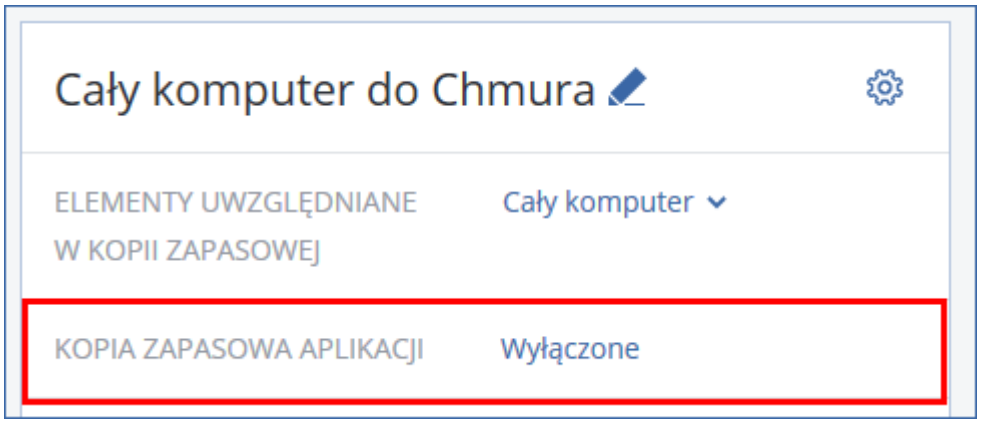
   Kliknij dwukrotnie komputer, aby wyświetlić znajdujące się na nim bazy danych (grupy magazynów).
3. Wybierz dane, które chcesz uwzględnić w kopii zapasowej. Jeśli pojawi się monit, podaj poświadczenia umożliwiające dostęp do danych.
4. Kliknij **Kopia zapasowa**.

Copyright © Acronis International GmbH, 2002-2017

11.3 Kopia zapasowa uwzględniająca aplikacje

Uwzględniająca aplikacje kopia zapasowa na poziomie dysku jest dostępna w przypadku komputerów fizycznych i maszyn wirtualnych ESXi.

W przypadku tworzenia kopii zapasowej komputera z programem Microsoft SQL Server, programem Microsoft Exchange Server lub usługami domenowymi Active Directory włącz **Kopia zapasowa aplikacji**, aby zyskać dodatkową ochronę danych tych aplikacji.



Dlaczego warto korzystać z kopii zapasowej uwzględniającej aplikacje?

Używanie kopii zapasowej uwzględniającej aplikacje przynosi następujące korzyści:

1. Aplikacje są uwzględniane w kopii zapasowej w spójnym stanie, dzięki czemu będą dostępne natychmiast po odzyskaniu maszyny.
2. Bazy danych SQL oraz bazy danych, skrzynki pocztowe i elementy skrzynek pocztowych programu Exchange można odzyskać bez odzyskiwania całej maszyny.
3. Po każdym pomyślnym utworzeniu kopii zapasowej są obcinane dzienniki transakcji SQL. Obcinanie dzienników SQL można wyłączyć w opcjach planu tworzenia kopii zapasowych (s. 62). Dzienniki transakcji programu Exchange są obcinane tylko na maszynach wirtualnych. Jeśli dzienniki transakcji programu Exchange mają być obcinane na komputerze fizycznym, włącz Pełne kopie zapasowe z usługą VSS (s. 70).
4. Jeśli domena zawiera więcej niż jeden kontroler domeny i jeden z nich zostanie odzyskany, wykonywane jest przywracanie nieautorytatywne i po odzyskaniu nie nastąpi wycofanie numeru USN.

Co jest potrzebne do skorzystania z kopii zapasowej uwzględniającej aplikacje?

Na komputerze fizycznym oprócz agenta dla systemu Windows musi być zainstalowany agent dla SQL i/lub agent dla programu Exchange. W przypadku maszyny wirtualnej nie jest wymagana instalacja żadnego agenta — zakłada się, że kopia zapasowa maszyny jest tworzona przez agenta dla VMware (w systemie Windows).

Inne wymagania podano w sekcjach „Wymagania wstępne” (s. 109) i „Wymagane prawa użytkownika” (s. 112).

11.3.1 Wymagane prawa użytkownika

Kopia zapasowa uwzględniająca aplikacje zawiera metadane znajdujących się na dysku aplikacji uwzględniających usługę VSS. Aby uzyskać dostęp do tych metadanych, agent potrzebuje konta z

Copyright © Acronis International GmbH, 2002-2017

odpowiednimi prawami. Wymieniono je poniżej. Podczas włączania tworzenia kopii zapasowej aplikacji pojawi się monit o określenie tego konta.

- W przypadku programu SQL Server:

  Konto musi należeć do grupy **Operatorzy kopii zapasowych** lub **Administratorzy** na danym komputerze oraz do roli **administratora systemu** w każdej instancji uwzględnianej w kopii zapasowej.
- W przypadku programu Exchange Server:

  Program Exchange 2007: Konto musi należeć do grupy roli **Administratorzy organizacji korzystającej z programu Exchange**.

  Program Exchange 2010 lub nowszy: Konto musi należeć do grupy roli **Zarządzanie organizacją**.
- W przypadku usługi Active Directory:

  Konto musi być administratorem domeny.

11.4 Odzyskiwanie baz danych SQL

W tej sekcji opisano odzyskiwanie z kopii zapasowych baz danych oraz kopii zapasowych uwzględniających aplikacje.

Bazy danych SQL można odzyskiwać do instancji serwera SQL pod warunkiem, że na komputerze z tą instancją jest zainstalowany agent dla SQL. Trzeba będzie podać poświadczenia konta należącego do grupy **Operatorzy kopii zapasowych** lub **Administratorzy** na danym komputerze oraz do roli **administratora systemu** w instancji docelowej.

Można też odzyskać bazy danych jako pliki. Może się to przydać w przypadku, gdy trzeba odzyskać bazy danych na komputer, na którym nie jest zainstalowany agent dla SQL, lub gdy trzeba wyodrębnić dane w celu ich wydobycia, inspekcji lub dalszego przetworzenia przy użyciu narzędzi innych producentów. Można dołączyć pliki bazy danych SQL do instancji serwera SQL zgodnie z instrukcjami podanymi w sekcji „Dołączanie baz danych programu SQL Server” (s. 115).

Jeśli używasz tylko agenta dla VMware, jedyną dostępną metodą odzyskiwania jest odzyskiwanie baz danych jako plików.

Systemowe bazy danych są odzyskiwane zasadniczo tak samo jak bazy danych użytkowników. Szczegóły charakteryzujące odzyskiwanie systemowych baz danych przedstawiono w sekcji „Odzyskiwanie systemowych baz danych” (s. 114).

Aby odzyskać bazy danych SQL

1. W przypadku odzyskiwania z kopii zapasowej bazy danych kliknij **Microsoft SQL**. W przeciwnym razie pomiń ten krok.
2. Wybierz komputer, który pierwotnie zawierał dane do odzyskania.
3. Kliknij **Odzyskiwanie**.
4. Wybierz punkt odzyskiwania. Uwaga: punkty odzyskiwania są filtrowane na podstawie lokalizacji.

   Jeśli komputer jest w trybie offline, punkty odzyskiwania nie są wyświetlane. Wykonaj jedną z następujących czynności:

   - Jeśli lokalizacją kopii zapasowych jest chmura lub współużytkowany magazyn (czyli magazyn, do którego mają dostęp inne agenty), kliknij **Wybierz komputer**, wybierz komputer z agentem dla SQL i wybierz punkt odzyskiwania.
   - Wybierz punkt odzyskiwania na karcie Kopie zapasowe (s. 92).

   Komputer wybrany do przeglądania w ramach jednej z powyższych czynności staje się komputerem docelowym odzyskiwania baz danych SQL.

 Copyright © Acronis International GmbH, 2002-2017

5. Wykonaj jedną z następujących czynności:
   - W przypadku odzyskiwania z kopii zapasowej bazy danych kliknij **Odzyskaj bazy danych SQL**.
   - W przypadku odzyskiwania z kopii zapasowej uwzględniającej aplikacje kliknij **Odzyskaj** > **Bazy danych SQL**.
6. Wybierz dane, które chcesz odzyskać. Kliknij dwukrotnie wybraną instancję, aby wyświetlić zawarte w niej bazy danych.
7. Jeśli chcesz odzyskać bazy danych jako pliki, kliknij **Odzyskaj jako pliki**, wybierz folder lokalny lub sieciowy, w którym mają zostać zapisane pliki, a następnie kliknij **Odzyskaj**. W przeciwnym razie pomiń ten krok.
8. Kliknij **Odzyskaj**.
9. Domyślnie program odzyska bazy danych do pierwotnej lokalizacji. Jeśli pierwotna baza danych nie istnieje, zostanie odtworzona. Możesz wybrać inny komputer lub inną instancję serwera SQL, gdzie mają zostać odzyskane bazy danych.

   Aby odzyskać bazę danych jako inną bazę danych w tej samej instancji:

   a. Kliknij nazwę bazy danych.
   b. W polu **Odzyskaj do** wybierz **Nowa baza danych**.
   c. Określ nazwę nowej bazy danych.
   d. Określ ścieżkę nowej bazy danych oraz ścieżkę dziennika. Określony tutaj folder nie może zawierać pierwotnej bazy danych ani plików dziennika.
10. [Opcjonalnie] Aby zmienić stan bazy danych po odzyskaniu, kliknij nazwę tej bazy i wybierz jeden z następujących stanów:
    - **Gotowe do użycia (PRZYWRACANIE Z ODZYSKIWANIEM)** (domyślny)

      Po zakończeniu odzyskiwania baza danych będzie gotowa do użycia. Użytkownicy będą mieli do niej pełny dostęp. Program cofnie wszystkie niezatwierdzone transakcje odzyskanej bazy danych zapisane w dziennikach transakcji. Odzyskanie dodatkowych dzienników transakcji z macierzystych kopii zapasowych programu Microsoft SQL będzie niemożliwe.
    - **Niegotowe do użycia (PRZYWRACANIE BEZ ODZYSKIWANIA)**

      Po zakończeniu odzyskiwania baza danych nie będzie gotowa do użycia. Użytkownicy nie będą mieli do niej dostępu. Program zachowa wszystkie niezatwierdzone transakcje odzyskanej bazy danych. Będzie możliwe odzyskanie dodatkowych dzienników transakcji z macierzystych kopii zapasowych programu Microsoft SQL, a tym samym osiągnięcie odpowiedniego punktu odzyskiwania.
    - **Tylko do odczytu (PRZYWRACANIE W STANIE GOTOWOŚCI)**

      Po zakończeniu odzyskiwania użytkownicy będą mieli dostęp tylko do odczytu do bazy danych. Program cofnie wszystkie niezatwierdzone transakcje. Zapisze jednak czynności cofania w tymczasowym pliku rezerwowym, aby było możliwe przywrócenie stanu sprzed odzyskania.

      Ta wartość jest używana głównie w celu wykrycia punktu w czasie, w którym wystąpił błąd programu SQL Server.
11. Kliknij **Rozpocznij odzyskiwanie**.

Postęp odzyskiwania jest widoczny na karcie **Działania**.

11.4.1 Odzyskiwanie systemowych baz danych

Program odzyska wszystkie systemowe bazy danych instancji jednocześnie. Podczas odzyskiwania systemowych baz danych oprogramowanie automatycznie uruchamia ponownie instancję docelową

Copyright © Acronis International GmbH, 2002-2017

w trybie jednego użytkownika. Po zakończeniu odzyskiwania program uruchamia ponownie instancję i odzyskuje pozostałe bazy danych (jeśli występują).

Pozostałe czynniki, które należy uwzględnić podczas odzyskiwania systemowych baz danych:

- Systemowe bazy danych można odzyskać tylko do instancji o takiej samej wersji jak pierwotna instancja.
- Systemowe bazy danych zawsze są odzyskiwane w stanie „gotowe do użycia".

Odzyskiwanie bazy danych master

Systemowe bazy danych obejmują bazę danych **master**. W bazie danych **master** rejestrowane są informacje na temat wszystkich baz danych w danej instancji. Dlatego baza danych **master** w kopii zapasowej zawiera informacje na temat baz danych istniejących w instancji w momencie utworzenia kopii zapasowej. Po odzyskaniu bazy danych **master** konieczne może być wykonanie następujących czynności:

- Bazy danych, które pojawiły się w instancji po utworzeniu kopii zapasowej, nie są dla tej instancji widoczne. Aby umożliwić używanie tych baz danych, dołącz je do instancji ręcznie przy użyciu programu SQL Server Management Studio.
- Bazy danych usunięte po utworzeniu kopii zapasowej są wyświetlane w instancji jako bazy w trybie offline. Usuń je przy użyciu programu SQL Server Management Studio.

11.4.2 Dołączanie baz danych programu SQL Server

W tej sekcji opisano sposób dołączania bazy danych w programie SQL Server za pomocą programu SQL Server Management Studio. W danej chwili może być dołączona tylko jedna baza danych.

Dołączenie bazy danych wymaga posiadania dowolnych z następujących uprawnień: **CREATE DATABASE**, **CREATE ANY DATABASE** lub **ALTER ANY DATABASE**. Zwykle uprawnienia te są przyznawane roli **administratora systemu** w ramach instancji.

Aby dołączyć bazę danych

1. Uruchom program Microsoft SQL Server Management Studio.
2. Podłącz żądaną instancję serwera SQL i rozwiń ją.
3. Prawym przyciskiem myszy kliknij **Bazy danych** i kliknij **Dołącz**.
4. Kliknij **Dodaj**.
5. W oknie dialogowym **Odszukaj pliki bazy danych** znajdź i wybierz plik .mdf file bazy danych.
6. W sekcji **Szczegóły bazy danych** sprawdź, czy pozostałe pliki bazy danych (pliki .ndf i .ldf) zostały znalezione.

   Informacje szczegółowe. Automatyczne znalezienie plików baz danych programu SQL może być niemożliwe, jeśli:

   - Nie znajdują się one w lokalizacji domyślnej ani w tym samym folderze co podstawowy plik bazy danych (.mdf). Rozwiązanie: ręcznie określ ścieżkę do wymaganych plików w kolumnie **Bieżąca ścieżka plików**.
   - Odzyskano niekompletny zestaw plików składających się na bazę danych. Rozwiązanie: odzyskaj z kopii zapasowej brakujące pliki bazy danych programu SQL Server.
7. Gdy znalezione zostaną wszystkie pliki, kliknij **OK**.

Copyright © Acronis International GmbH, 2002-2017

11.5 Odzyskiwanie baz danych programu Exchange

W tej sekcji opisano odzyskiwanie z kopii zapasowych baz danych oraz kopii zapasowych uwzględniających aplikacje.

Dane programu Exchange Server można odzyskać na działający serwer Exchange. Może to być pierwotny serwer Exchange lub serwer Exchange w tej samej wersji działający na komputerze o takiej samej w pełni kwalifikowanej nazwie domeny. Na komputerze docelowym musi być zainstalowany agent dla programu Exchange.

Poniższa tabela zawiera zestawienie danych programu Exchange Server, które można wybrać do odzyskania, oraz minimalne prawa użytkownika wymagane w celu odzyskania tych danych.

Wersja programu Exchange	Elementy danych	Prawa użytkownika
2007	Grupy magazynów	Członkostwo w grupie z rolą **Administratorzy organizacji korzystającej z programu Exchange**.
2010/2013/2016	Bazy danych	Członkostwo w grupie z rolą **Zarządzanie organizacją**.

Można też odzyskać bazy danych (grupy magazynów) jako pliki. Pliki baz danych oraz pliki dzienników transakcji zostaną wyodrębnione z kopii zapasowej do określonego folderu. Może się to przydać, gdy trzeba wyodrębnić dane do inspekcji lub dalszego przetwarzania przez narzędzia innych firm lub gdy odzyskiwanie z jakiegoś powodu się nie powiodło i potrzebny jest sposób na ręczne zamontowanie baz danych (s. 117).

Jeśli używasz tylko agenta dla VMware, jedyną dostępną metodą odzyskiwania jest odzyskiwanie baz danych jako plików.

Aby odzyskać dane programu Exchange

W przypadku tej procedury pojęcie „bazy danych” dotyczy zarówno baz danych, jak i grup magazynów.

1. W przypadku odzyskiwania z kopii zapasowej bazy danych kliknij **Microsoft Exchange**. W przeciwnym razie pomiń ten krok.
2. Wybierz komputer, który pierwotnie zawierał dane do odzyskania.
3. Kliknij **Odzyskiwanie**.
4. Wybierz punkt odzyskiwania. Uwaga: punkty odzyskiwania są filtrowane na podstawie lokalizacji.

   Jeśli komputer jest w trybie offline, punkty odzyskiwania nie są wyświetlane. Skorzystaj z innych metod odzyskiwania:

   - Jeśli lokalizacją kopii zapasowych jest chmura lub współużytkowany magazyn (czyli magazyn, do którego mają dostęp inne agenty), kliknij **Wybierz komputer**, wybierz komputer z agentem dla programu Exchange i wybierz punkt odzyskiwania.
   - Wybierz punkt odzyskiwania na karcie Kopie zapasowe (s. 92).

   Komputer wybrany do przeglądania w ramach jednej z powyższych czynności staje się komputerem docelowym odzyskiwania danych programu Exchange.
5. Kliknij **Odzyskaj** > **Bazy danych programu Exchange**.
6. Wybierz dane, które chcesz odzyskać.
7. Jeśli chcesz odzyskać bazy danych jako pliki, kliknij **Odzyskaj jako pliki**, wybierz folder lokalny lub sieciowy, w którym mają zostać zapisane pliki, a następnie kliknij **Odzyskaj**. W przeciwnym razie pomiń ten krok.

Copyright © Acronis International GmbH, 2002-2017

8. Kliknij **Odzyskaj**. Jeśli pojawi się monit, podaj poświadczenia umożliwiające dostęp do programu Exchange Server.
9. Domyślnie program odzyska bazy danych do pierwotnej lokalizacji. Jeśli pierwotna baza danych nie istnieje, zostanie odtworzona.

   Aby odzyskać bazę danych jako inną bazę danych:

   a. Kliknij nazwę bazy danych.
   b. W polu **Odzyskaj do** wybierz **Nowa baza danych**.
   c. Określ nazwę nowej bazy danych.
   d. Określ ścieżkę nowej bazy danych oraz ścieżkę dziennika. Określony tutaj folder nie może zawierać pierwotnej bazy danych ani plików dziennika.
10. Kliknij **Rozpocznij odzyskiwanie**.

Postęp odzyskiwania jest widoczny na karcie **Działania**.

11.5.1 Montowanie baz danych programu Exchange Server

Po odzyskaniu plików baz danych można udostępnić bazy danych w trybie online, montując je. Montowanie przeprowadza się za pomocą konsoli Exchange Management Console, menedżera Exchange System Manager lub powłoki Exchange Management Shell.

Odzyskane bazy danych będą się znajdować w stanie „nieprawidłowego zamknięcia systemu”. Bazę danych będącą w stanie „nieprawidłowego zamknięcia systemu” może zamontować, jeśli zostanie ona odzyskana do oryginalnej lokalizacji (informacje o oryginalnej bazie danych są obecne w usłudze Active Directory). W przypadku odzyskiwania bazy danych do innej lokalizacji (np. nowej bazy danych lub bazy danych odzyskiwania) bazę tę można zamontować dopiero po doprowadzeniu jej do stanu „czystego zamknięcia” za pomocą polecenia **`Eseutil /r <Enn>`**. Nazwa **`<Enn>`** określa prefiks pliku dziennika bazy danych (lub grupy magazynów zawierającej bazę danych), względem której należy zastosować pliki dziennika transakcji.

Konto używane do dołączania bazy danych musi mieć delegowaną rolę administratora programu Exchange Server i lokalną grupę Administratorzy serwera docelowego.

Aby uzyskać więcej informacji na temat montowania baz danych, zobacz następujące artykuły:

- Program Exchange 2016: http://technet.microsoft.com/en-us/library/aa998871.aspx
- Program Exchange 2013: http://technet.microsoft.com/en-us/library/aa998871(v=EXCHG.150).aspx
- Program Exchange 2010: http://technet.microsoft.com/en-us/library/aa998871(v=EXCHG.141).aspx
- Program Exchange 2007: http://technet.microsoft.com/en-us/library/aa998871(v=EXCHG.80).aspx

11.6 Odzyskiwanie skrzynek pocztowych programu Exchange i ich elementów

W tej sekcji opisano, jak odzyskać skrzynki pocztowe programu Exchange i ich elementy z kopii zapasowych baz danych oraz kopii zapasowych uwzględniających aplikacje.

Copyright © Acronis International GmbH, 2002-2017

Omówienie

Odzyskiwanie granularne jest możliwe tylko w przypadku programu Microsoft Exchange Server 2010 z dodatkiem Service Pack 1 (SP1) lub nowszego. Źródłowa kopia zapasowa może zawierać bazy danych dowolnej obsługiwanej wersji programu Exchange.

Odzyskiwanie granularne może wykonać agent dla programu Exchange lub agent dla VMware (w systemie Windows). Docelowy komputer z programem Exchange Server oraz komputer z uruchomionym agentem muszą się znajdować w tym samym lesie usługi Active Directory.

Można odzyskać następujące elementy:

- Skrzynki pocztowe (z wyjątkiem archiwalnych skrzynek pocztowych)
- Foldery publiczne
- Elementy folderu publicznego
- Foldery poczty e-mail
- Wiadomości e-mail
- Zdarzenia kalendarza
- Zadania
- Kontakty
- Wpisy dziennika
- Notatki

Elementy można znaleźć przy użyciu funkcji wyszukiwania.

W przypadku odzyskiwania skrzynki pocztowej do już istniejącej skrzynki dostępne w niej elementy o takich samych identyfikatorach zostaną zastąpione.

Odzyskiwanie elementów skrzynki pocztowej nie powoduje zastępowania żadnych danych. Elementy skrzynki pocztowej są zawsze odzyskiwane do folderu **Odzyskane elementy** docelowej skrzynki pocztowej.

Wymagania dotyczące kont użytkowników

Odzyskiwana z kopii zapasowej skrzynka pocztowa musi mieć powiązane konto użytkownika w usłudze Active Directory.

Skrzynki pocztowe użytkowników i ich zawartość można odzyskać tylko pod warunkiem, że są *włączone* powiązane z nimi konta użytkowników. Współdzielone skrzynki pocztowe oraz skrzynki pocztowe pomieszczeń i urządzeń można odzyskać pod warunkiem, że powiązane z nimi konta użytkowników są *wyłączone*.

Skrzynki pocztowe, które nie spełniają powyższych warunków, są pomijane podczas odzyskiwania.

W przypadku pominięcia niektórych skrzynek pocztowych odzyskiwanie zakończy się powodzeniem z ostrzeżeniami. W przypadku pominięcia wszystkich skrzynek pocztowych odzyskiwania zakończy się niepowodzeniem.

11.6.1 Odzyskiwanie skrzynek pocztowych

1. W przypadku odzyskiwania z kopii zapasowej bazy danych kliknij **Microsoft Exchange**. W przeciwnym razie pomiń ten krok.
2. Wybierz komputer, który pierwotnie zawierał dane do odzyskania.
3. Kliknij **Odzyskiwanie**.

Copyright © Acronis International GmbH, 2002-2017

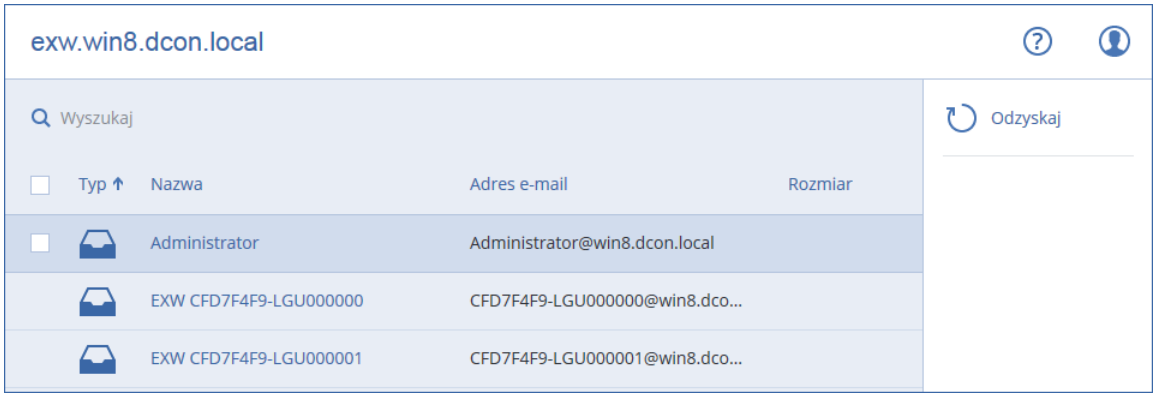
4. Wybierz punkt odzyskiwania. Uwaga: punkty odzyskiwania są filtrowane na podstawie lokalizacji.

   Jeśli komputer jest w trybie offline, punkty odzyskiwania nie są wyświetlane. Skorzystaj z innych metod odzyskiwania:

   - Jeśli lokalizacją kopii zapasowych jest chmura lub współużytkowany magazyn (czyli magazyn, do którego mają dostęp inne agenty), kliknij **Wybierz komputer**, wybierz komputer z agentem dla VMware i wybierz punkt odzyskiwania.
   - Wybierz punkt odzyskiwania na karcie Kopie zapasowe (s. 92).

   Komputer wybrany do przejrzenia w ramach dowolnego z powyższych działań wykona operację odzyskiwania w zastępstwie pierwotnego komputera będącego w trybie offline.
5. Kliknij **Odzyskaj** > **Skrzynki pocztowe programu Exchange**.
6. Wybierz skrzynki pocztowe, które chcesz odzyskać.

   Skrzynki pocztowe można wyszukiwać według nazwy. Symbole wieloznaczne nie są obsługiwane.



7. Kliknij **Odzyskaj**.
8. Kliknij **Komputer docelowy z programem Microsoft Exchange Server**, aby wybrać lub zmienić komputer docelowy. Dzięki temu można odzyskać dane na komputer bez agenta dla programu Exchange.

   Określ w pełni kwalifikowaną nazwę domeny (FQDN) komputera, na którym jest włączona rola **Dostęp klienta** programu Microsoft Exchange Server. Komputer musi należeć do tego samego lasu usługi Active Directory co komputer wykonujący operację odzyskiwania.

   Jeśli pojawi się stosowny monit, podaj poświadczenia konta należącego do grupy roli **Zarządzanie organizacją**.
9. [Opcjonalnie] Kliknij **Baza danych używana do odtworzenia brakujących skrzynek pocztowych**, aby zmienić automatycznie wybraną bazę danych.
10. Kliknij **Rozpocznij odzyskiwanie**.
11. Potwierdź decyzję.

Postęp odzyskiwania jest widoczny na karcie **Działania**.

11.6.2 Odzyskiwanie elementów skrzynki pocztowej

1. W przypadku odzyskiwania z kopii zapasowej bazy danych kliknij **Microsoft Exchange**. W przeciwnym razie pomiń ten krok.
2. Wybierz komputer, który pierwotnie zawierał dane do odzyskania.
3. Kliknij **Odzyskiwanie**.
4. Wybierz punkt odzyskiwania. Uwaga: punkty odzyskiwania są filtrowane na podstawie lokalizacji.

   Jeśli komputer jest w trybie offline, punkty odzyskiwania nie są wyświetlane. Skorzystaj z innych metod odzyskiwania:

Copyright © Acronis International GmbH, 2002-2017

- Jeśli lokalizacją kopii zapasowych jest chmura lub współużytkowany magazyn (czyli magazyn, do którego mają dostęp inne agenty), kliknij **Wybierz komputer**, wybierz komputer z agentem dla VMware i wybierz punkt odzyskiwania.
- Wybierz punkt odzyskiwania na karcie Kopie zapasowe (s. 92).

Komputer wybrany do przejrzenia w ramach dowolnego z powyższych działań wykona operację odzyskiwania w zastępstwie pierwotnego komputera będącego w trybie offline.

5. Kliknij **Odzyskaj** > **Skrzynki pocztowe programu Exchange**.
6. Kliknij skrzynkę pocztową, która pierwotnie zawierała elementy do odzyskania.
7. Wybierz elementy, które chcesz odzyskać.

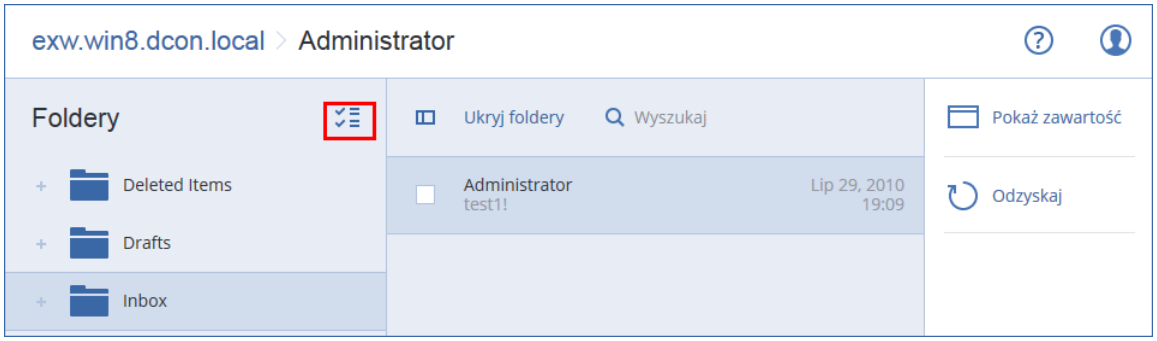
   Dostępne są poniższe opcje wyszukiwania. Symbole wieloznaczne nie są obsługiwane.

   - Wiadomości e-mail: wyszukiwanie według tematu, nadawcy, adresata i daty.
   - Zdarzenia: wyszukiwanie według tematu i daty.
   - Zadania: wyszukiwanie według tematu i daty.
   - Kontakty: wyszukiwanie według nazwiska (nazwy), adresu e-mail i numeru telefonu.

   Po zaznaczeniu wiadomości e-mail możesz kliknąć **Pokaż zawartość**, aby wyświetlić jej zawartość, w tym załączniki.

   Wskazówka *Kliknij nazwę załączonego pliku, aby go pobrać.*

   Aby mieć możliwość wybrania folderów, kliknij ikonę odzyskiwania folderów.



8. Kliknij **Odzyskaj**.
9. Kliknij **Komputer docelowy z programem Microsoft Exchange Server**, aby wybrać lub zmienić komputer docelowy. Dzięki temu można odzyskać dane na komputer bez agenta dla programu Exchange.

   Określ w pełni kwalifikowaną nazwę domeny (FQDN) komputera, na którym jest włączona rola **Dostęp klienta** programu Microsoft Exchange Server. Komputer musi należeć do tego samego lasu usługi Active Directory co komputer wykonujący operację odzyskiwania.

   Jeśli pojawi się stosowny monit, podaj poświadczenia konta należącego do grupy roli **Zarządzanie organizacją**.
10. W polu **Docelowa skrzynka pocztowa** wyświetl, zmień lub określ docelową skrzynkę pocztową.

    Domyślnie jest wybierana pierwotna skrzynka pocztowa. Jeśli ta skrzynka pocztowa nie istnieje lub wybrano komputer inny niż pierwotny, trzeba określić docelową skrzynkę pocztową.
11. Kliknij **Rozpocznij odzyskiwanie**.
12. Potwierdź decyzję.

Postęp odzyskiwania jest widoczny na karcie **Działania**.

Copyright © Acronis International GmbH, 2002-2017

12 Ochrona skrzynek pocztowych Office 365

Dlaczego warto tworzyć kopie zapasowe skrzynek pocztowych Office 365?

Choć Microsoft Office 365 jest usługą chmurową, regularne kopie zapasowe stanowią dodatkową warstwę ochrony przed błędami popełnianymi przez użytkowników oraz celowo złośliwymi działaniami. Usunięte elementy można odzyskać z kopii zapasowej nawet po upływie okresu ich przechowywania w usłudze Office 365. Można też przechowywać lokalną kopię skrzynek pocztowych Office 365, jeśli wymagają tego obowiązujące regulacje.

Co jest potrzebne do utworzenia kopii zapasowej skrzynek pocztowych?

Aby móc utworzyć kopię zapasową skrzynek pocztowych Office 365 i je odzyskać, trzeba mieć przypisaną rolę administratora globalnego w usłudze Microsoft Office 365.

Zainstaluj agenta dla usługi Office 365 na podłączonym do Internetu komputerze z systemem Windows. W organizacji musi się znajdować tylko jeden agent dla usługi Office 365. W przypadku wdrożenia chmurowego agent musi być zarejestrowany na koncie administratora najwyższego poziomu (administratora klienta).

- W przypadku wdrożenia chmurowego wprowadź poświadczenia administratora klienta podczas instalacji agenta oraz logowania się do interfejsu internetowego.
- Na stronie **Microsoft Office 365** w interfejsie internetowym wprowadź poświadczenia administratora globalnego usługi Office 365.

  Agent zaloguję się do usługi Office 365 przy użyciu tego konta. Aby umożliwić agentowi dostęp do zawartości wszystkich skrzynek pocztowych, kontu temu zostanie przypisana rola zarządzania **ApplicationImpersonation**.

Jakie elementy można odzyskać?

Z kopii zapasowej skrzynek pocztowych można odzyskać następujące elementy:

- Skrzynki pocztowe
- Foldery poczty e-mail
- Wiadomości e-mail
- Zdarzenia kalendarza
- Zadania
- Kontakty
- Wpisy dziennika
- Notatki

Elementy można znaleźć przy użyciu funkcji wyszukiwania.

W przypadku odzyskiwania skrzynki pocztowej do już istniejącej skrzynki dostępne w niej elementy o takich samych identyfikatorach zostaną zastąpione.

Odzyskiwanie elementów skrzynki pocztowej nie powoduje zastępowania żadnych danych. Elementy skrzynki pocztowej są zawsze odzyskiwane do folderu **Odzyskane elementy** docelowej skrzynki pocztowej.

Ograniczenia

- Nie można tworzyć kopii zapasowych archiwalnych skrzynek pocztowych (**archiwum zbiorczego**).

Copyright © Acronis International GmbH, 2002-2017

- Nie można odzyskać danych do nowej skrzynki pocztowej. Najpierw trzeba ręcznie utworzyć nowego użytkownika usługi Office 365, a następnie odzyskać elementy do jego skrzynki pocztowej.
- Odzyskiwanie do innej organizacji w usłudze Microsoft Office 365 lub lokalnej instancji programu Microsoft Exchange Server nie jest obsługiwane.

12.1 Wybieranie skrzynek pocztowych Office 365

Wybierz skrzynki pocztowe zgodnie z poniższymi instrukcjami, a następnie określ w odpowiedni sposób (s. 42) ustawienia planu tworzenia kopii zapasowych.

Aby wybrać skrzynki pocztowe Microsoft Office 365

1. Kliknij **Microsoft Office 365**.
2. Jeśli pojawi się taki monit, zaloguj się do usługi Microsoft Office 365 jako administrator globalny.
3. Wybierz skrzynki pocztowe, które chcesz uwzględnić w kopii zapasowej.
4. Kliknij **Kopia zapasowa**.

12.2 Odzyskiwanie skrzynek pocztowych Office 365 i ich elementów

12.2.1 Odzyskiwanie skrzynek pocztowych

1. Kliknij **Microsoft Office 365**.
2. Wybierz skrzynkę pocztową do odzyskania, a następnie kliknij **Odzyskiwanie**.

   Skrzynki pocztowe można wyszukiwać według nazwy. Symbole wieloznaczne nie są obsługiwane.

   Jeśli skrzynka pocztowa została usunięta, wybierz ją na karcie Kopie zapasowe (s. 92), a następnie kliknij **Pokaż kopie zapasowe**.
3. Wybierz punkt odzyskiwania. Uwaga: punkty odzyskiwania są filtrowane na podstawie lokalizacji.
4. Kliknij **Odzyskaj** > **Skrzynka pocztowa**.
5. W polu **Docelowa skrzynka pocztowa** wyświetl, zmień lub określ docelową skrzynkę pocztową.

   Domyślnie jest wybierana pierwotna skrzynka pocztowa. Jeśli tej skrzynki pocztowej już nie ma, trzeba określić docelową skrzynkę pocztową.
6. Kliknij **Rozpocznij odzyskiwanie**.

12.2.2 Odzyskiwanie elementów skrzynki pocztowej

1. Kliknij **Microsoft Office 365**.
2. Wybierz skrzynkę pocztową, która pierwotnie zawierała elementy do odzyskania, a następnie kliknij **Odzyskiwanie**.

   Skrzynki pocztowe można wyszukiwać według nazwy. Symbole wieloznaczne nie są obsługiwane.

   Jeśli skrzynka pocztowa została usunięta, wybierz ją na karcie Kopie zapasowe (s. 92), a następnie kliknij **Pokaż kopie zapasowe**.
3. Wybierz punkt odzyskiwania. Uwaga: punkty odzyskiwania są filtrowane na podstawie lokalizacji.
4. Kliknij **Odzyskaj** > **Wiadomości e-mail**.
5. Wybierz elementy, które chcesz odzyskać.

   Dostępne są poniższe opcje wyszukiwania. Symbole wieloznaczne nie są obsługiwane.

   - Wiadomości e-mail: wyszukiwanie według tematu, nadawcy, adresata i daty.

Copyright © Acronis International GmbH, 2002-2017

- Zdarzenia: wyszukiwanie według tematu i daty.
- Zadania: wyszukiwanie według tematu i daty.
- Kontakty: wyszukiwanie według nazwiska (nazwy), adresu e-mail i numeru telefonu.

Po zaznaczeniu wiadomości e-mail możesz kliknąć **Pokaż zawartość**, aby wyświetlić jej zawartość, w tym załączniki.

Wskazówka *Kliknij nazwę załączonego pliku, aby go pobrać.*

Po zaznaczeniu wiadomości e-mail możesz kliknąć **Wyślij jako wiadomość e-mail**, aby wysłać wiadomość na jakiś adres e-mail. Wiadomość zostanie wysłana z adresu email konta administratora.

Aby mieć możliwość wybrania folderów, kliknij ikonę „Odzyskaj foldery”: 

6. Kliknij **Odzyskaj**.
7. W polu **Docelowa skrzynka pocztowa** wyświetl, zmień lub określ docelową skrzynkę pocztową.

   Domyślnie jest wybierana pierwotna skrzynka pocztowa. Jeśli tej skrzynki pocztowej już nie ma, trzeba określić docelową skrzynkę pocztową.
8. Kliknij **Rozpocznij odzyskiwanie**.
9. Potwierdź decyzję.

Elementy skrzynki pocztowej są zawsze odzyskiwane do folderu **Odzyskane elementy** docelowej skrzynki pocztowej.

13 Zaawansowane operacje dotyczące maszyn wirtualnych

13.1 Uruchamianie maszyny wirtualnej z kopii zapasowej (Instant Restore)

Maszynę wirtualną można uruchomić z kopii zapasowej na poziomie dysku, która zawiera system operacyjny. Operacja ta, nazywana również odzyskiwaniem błyskawicznym, umożliwia przygotowanie serwera wirtualnego w kilka sekund. Dyski wirtualne są emulowane bezpośrednio z kopii zapasowej, dzięki czemu nie zajmują miejsca w magazynie danych (magazynie). Miejsce w pamięci masowej jest wymagane wyłącznie w celu przechowywania zmian zachodzących na dyskach wirtualnych.

Taka tymczasowa maszyna wirtualna powinna działać przez maksymalnie trzy dni. Po tym czasie można ją całkowicie usunąć lub przekształcić w zwykłą maszynę wirtualną (sfinalizować) bez przerywania jej działania.

Dopóki istnieje tymczasowa maszyna wirtualna, do używanej przez nią kopii zapasowej nie można stosować reguł przechowywania. Operacje tworzenia kopii zapasowych pierwotnej maszyny mogą być nadal uruchamiane.

Przykłady użycia

- **Odzyskiwanie po awarii**

  Można niezwłocznie udostępnić kopię uszkodzonej maszyny wirtualnej w trybie online.
- **Testowanie kopii zapasowych**

Copyright © Acronis International GmbH, 2002-2017

Można uruchomić maszynę z kopii zapasowej i upewnić się, czy system operacyjny-gość i aplikacje działają prawidłowo.

- **Uzyskiwanie dostępu do danych aplikacji**

  W czasie działania maszyny można ocenić i wyodrębnić wymagane dane przy użyciu macierzystych narzędzi do zarządzania aplikacji.

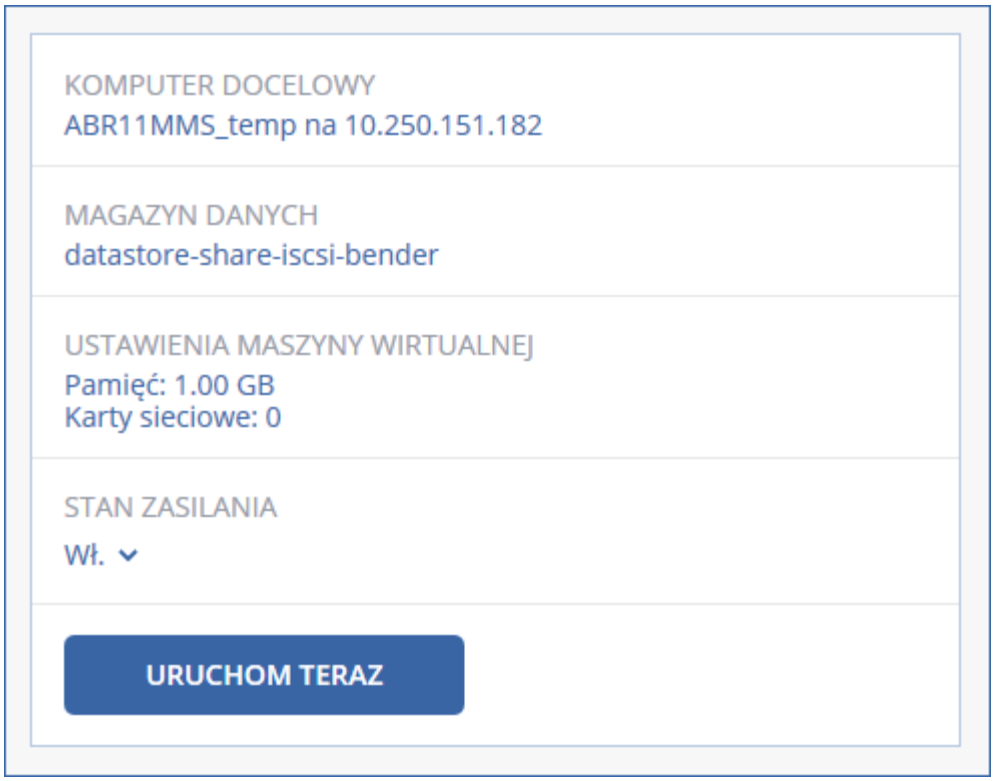
Wymagania wstępne

- W usłudze kopii zapasowych musi być zarejestrowany co najmniej jeden agent dla VMware lub agent dla Hyper-V.
- Kopia zapasowa może być przechowywana w folderze sieciowym lub folderze lokalnym komputera z zainstalowanym agentem dla VMware lub agentem dla Hyper-V. Jeśli wybierzesz folder sieciowy, musi on być dostępny z danego komputera. Maszynę wirtualną można też uruchomić z kopii zapasowej przechowywanej w chmurze, ale wtedy będzie ona działać wolniej, ponieważ operacja ta wymaga intensywnych operacji odczytu losowego z kopii zapasowej.
- Kopia zapasowa musi zawierać cały komputer lub wszystkie woluminy wymagane do uruchomienia systemu operacyjnego.
- Można korzystać z kopii zapasowych zarówno komputerów fizycznych, jak i maszyn wirtualnych. Nie można korzystać z kopii zapasowych *kontenerów* Virtuozzo.

13.1.1 Uruchamianie maszyny

1. Wykonaj jedną z następujących czynności:
   - Wybierz komputer objęty operacją tworzenia kopii zapasowej, kliknij **Odzyskaj**, a następnie wybierz punkt odzyskiwania.
   - Wybierz punkt odzyskiwania na karcie Kopie zapasowe (s. 92).
2. Kliknij **Uruchom jako maszynę wirtualną**.

   Program automatycznie wybierze host i inne wymagane parametry.



Copyright © Acronis International GmbH, 2002-2017

3. [Opcjonalnie] Kliknij **Komputer docelowy**, a następnie zmień typ maszyny wirtualnej (ESXi lub Hyper-V), host lub nazwę maszyny wirtualnej.
4. [Optional] Kliknij **Magazyn danych** w przypadku ESXi lub **Ścieżka** w przypadku Hyper-V, a następnie wybierz magazyn danych dla maszyny wirtualnej.

   W czasie działania maszyny są gromadzone zmiany zachodzące na dyskach wirtualnych. Upewnij się, że w wybranym magazynie danych jest wystarczająco dużo wolnego miejsca.
5. [Opcjonalnie] Kliknij **Ustawienia maszyny wirtualnej**, aby zmienić rozmiar pamięci oraz połączenia sieciowe maszyny wirtualnej.
6. [Opcjonalnie] Wybierz stan zasilania maszyny (**Włączono**/**Wyłączono**).
7. Kliknij **Uruchom teraz**.

W efekcie maszyna będzie pokazywana w interfejsie internetowym z jedną z następujących ikon:  lub 

. Takich maszyn wirtualnych nie można wybierać do uwzględnienia w kopii zapasowej.

13.1.2 Usuwanie maszyny

Odradzamy usuwanie tymczasowych maszyn wirtualnych bezpośrednio w środowisku vSphere czy Hyper-V. Może to prowadzić do powstawania artefaktów w interfejsie internetowym. Ponadto, kopia zapasowa, z której została uruchomiona maszyna, może pozostać przez jakiś czas zablokowana (nie może zostać usunięta zgodnie z regułami przechowywania).

Aby usunąć maszynę wirtualną uruchomioną z kopii zapasowej

1. Na karcie **Wszystkie urządzenia** zaznacz maszynę uruchomioną z kopii zapasowej.
2. Kliknij **Usuń**.

Maszyna zostanie usunięta z interfejsu internetowego. Zostanie także usunięta z inwentaryzacji oraz magazynu danych (magazynu) vSphere lub Hyper-V. Wszelkie zmiany w danych wprowadzone w czasie działania maszyny zostaną utracone.

13.1.3 Finalizowanie maszyny

W przypadku uruchomienia maszyny wirtualnej z kopii zapasowej zawartość dysków wirtualnych jest pobierana bezpośrednio z tej kopii. Dlatego w przypadku utraty połączenia z lokalizacją kopii zapasowej lub agentem kopii zapasowej maszyna może przestać być dostępna lub nawet zostać uszkodzona.

W przypadku maszyny ESXi jest dostępna opcja przekształcenia maszyny w maszynę trwałą, tj. odzyskania wszystkich jej dysków wirtualnych, a także zmian, które zaszły w czasie działania maszyny, do magazynu danych przechowującego te zmiany. Proces ten określa się mianem finalizacji.

Finalizacja jest wykonywana bez przerywania działania. Maszyna wirtualna *nie* zostanie wyłączona w czasie finalizacji.

Aby sfinalizować maszynę uruchomioną z kopii zapasowej

1. Na karcie **Wszystkie urządzenia** zaznacz maszynę uruchomioną z kopii zapasowej.
2. Kliknij **Finalizuj**.
3. [Opcjonalnie] Określ nową nazwę maszyny.
4. [Opcjonalnie] Zmień tryb alokowania dysku. Ustawienie domyślne to **Elastyczne**.

Copyright © Acronis International GmbH, 2002-2017

5. Kliknij **Finalizuj**.

Nazwa maszyny zostanie natychmiast zmieniona. Postęp odzyskiwania będzie widoczny na karcie **Działania**. Po ukończeniu odzyskiwania ikona maszyny zostanie zastąpiona ikoną zwykłej maszyny wirtualnej.

13.2 Replikacja maszyn wirtualnych

Replikacja jest dostępna tylko w przypadku maszyn wirtualnych VMware ESXi.

Proces replikacji polega na utworzeniu dokładnej kopii (repliki) maszyny wirtualnej, a następnie ciągłym synchronizowaniu repliki z pierwotną maszyną. Dzięki replikowaniu krytycznej maszyny wirtualnej zawsze będziesz dysponować gotową do uruchomienia kopią tej maszyny.

Replikację można rozpocząć ręcznie lub zgodnie z samodzielnie określonym harmonogramem. Pierwsza replikacja jest pełna (polega na utworzeniu kopii całej maszyny). Kolejne replikacje są przyrostowe. Wykonuje się je przy użyciu funkcji Changed Block Tracking (s. 129), chyba że ta opcja jest wyłączona.

Replikacja a tworzenie kopii zapasowej

W odróżnieniu od zaplanowanych kopii zapasowych replika przechowuje tylko ostatni stan maszyny wirtualnej. Replika zajmuje miejsce w magazynie danych, podczas gdy kopii zapasowe można przechowywać w tańszym magazynie.

Z drugiej strony włączenie repliki trwa znacznie krócej niż operacja odzyskiwania i krócej niż uruchomienie maszyny wirtualnej z kopii zapasowej. Włączona replika działa znacznie szybciej niż maszyna wirtualna uruchomiona z kopii zapasowej i nie wymaga załadowania agenta dla VMware.

Przykłady użycia

- **Replikacja maszyny wirtualnej do lokalizacji zdalnej.**

  Replikacja pozwala na normalne funkcjonowanie w warunkach częściowej lub całkowitej awarii centrum danych dzięki sklonowaniu maszyn wirtualnych z lokalizacji podstawowej do dodatkowej. Lokalizacja dodatkowa zwykle znajduje się w innym obiekcie, któremu raczej nie zagraża problem środowiskowy czy infrastrukturowy ani żadne inne czynniki będące przyczyną ewentualnej awarii w lokalizacji podstawowej.
- **Replikacja maszyn wirtualnych w ramach jednej lokalizacji (z jednego hosta / magazynu danych do drugiego).**

  Replikację lokalną można stosować na potrzeby wysokiej dostępności lub odzyskiwania po awarii.

Możliwe zadania związane z repliką

- **Testowanie repliki** (s. 128)

  W celu przeprowadzenia testów replika zostanie włączona. Wówczas za pomocą klienta vSphere lub innych narzędzi należy sprawdzić, czy replika działa prawidłowo. Na czas testów replikacja zostanie zawieszona.
- **Przełączenie awaryjne na replikę** (s. 128)

  Przełączenie awaryjne polega na przeniesieniu obciążenia z pierwotnej maszyny wirtualnej na jej replikę. Na czas przełączenia awaryjnego replikacja zostanie zawieszona.
- **Tworzenie kopii zapasowej repliki**

  Operacje tworzenia kopii zapasowych i replikacji wymagają dostępu do dysków wirtualnych, w związku z czym obniżają wydajność hosta, na którym działa maszyna wirtualna. Jeśli chcesz mieć zarówno replikę, jak i kopie zapasowe maszyny wirtualnej, ale nie chcesz dodatkowo obciążać

Copyright © Acronis International GmbH, 2002-2017

hosta produkcyjnego, zreplikuj maszynę na inny host i skonfiguruj tworzenie kopii zapasowych repliki.

Ograniczenia

Nie można replikować maszyn wirtualnych następujących typów:

- Maszyny odporne na awarie w środowisku ESXi w wersji 5.5 lub starszej
- Maszyny uruchomione z kopii zapasowych
- Repliki maszyn wirtualnych

13.2.1 Tworzenie planu replikacji

Plan replikacji trzeba utworzyć dla każdego komputera z osobna. Nie można zastosować istniejącego już planu do innych komputerów.

Aby utworzyć plan replikacji

1. Wybierz maszynę wirtualną do replikacji.
2. Kliknij **Replikacja**.

   W oprogramowaniu zostanie wyświetlony nowy szablon planu replikacji.
3. [Opcjonalnie] Aby zmodyfikować nazwę planu replikacji, kliknij nazwę domyślną.
4. Kliknij **Komputer docelowy**, a następnie zrób tak:
   a. Wybierz, czy ma zostać utworzona nowa replika, czy chcesz użyć istniejącej już repliki pierwotnego komputera.
   b. Wybierz host ESXi i określ nazwę nowej repliki lub wybierz replikę już istniejącą.

      Domyślnie nowa replika ma nazwę **[Nazwa pierwotnego komputera]_replica**.
   c. Kliknij **OK**.
5. [Tylko w przypadku replikacji na nową maszynę] Kliknij **Magazyn danych** i wybierz magazyn danych dla maszyny wirtualnej.
6. [Opcjonalnie] Kliknij **Harmonogram**, aby zmienić harmonogram replikacji.

   Domyślnie replikacje są wykonywane codziennie od poniedziałku do piątku. Można wybrać godzinę rozpoczęcia replikacji.

   Aby zmienić częstość replikacji, przesuń suwak i określ harmonogram.

   Możesz też:
   - Określić zakres dat wyznaczający okres obowiązywania harmonogramu. Zaznacz pole wyboru **Uruchom plan w danym przedziale dat**, a następnie określ zakres dat.
   - Wyłączyć harmonogram. W tym przypadku replikację można rozpocząć ręcznie.
7. [Opcjonalnie] Kliknij ikonę koła zębatego, aby zmodyfikować opcje replikacji (s. 129).
8. Kliknij **Zastosuj**.
9. [Opcjonalnie] Aby uruchomić plan ręcznie, kliknij **Uruchom teraz** w panelu planu.

W wyniku uruchomienia planu replikacji replika maszyny wirtualnej pojawi się na liście **Wszystkie urządzenia** oznaczona następującą ikoną: 

Copyright © Acronis International GmbH, 2002-2017

13.2.2 Testowanie repliki

Aby przygotować replikę do testu

1. Wybierz replikę do przetestowania.
2. Kliknij **Testuj replikę**.
3. Kliknij **Rozpocznij testowanie**.
4. Wybierz, czy włączona replika ma zostać podłączona do sieci. Domyślnie replika nie będzie podłączona do sieci.
5. [Opcjonalnie] Jeśli zdecydujesz się na podłączenie repliki do sieci, zaznacz pole wyboru **Zatrzymaj oryginalną maszynę wirtualną**, aby zatrzymać pierwotny komputer, zanim włączysz replikę.
6. Kliknij **Rozpocznij**.

Aby zatrzymać testowanie repliki

1. Wybierz testowaną replikę.
2. Kliknij **Testuj replikę**.
3. Kliknij **Zatrzymaj testowanie**.
4. Potwierdź decyzję.

13.2.3 Przełączanie awaryjne na replikę

Aby przełączyć maszynę awaryjnie na replikę

1. Wybierz replikę docelową przełączania awaryjnego.
2. Kliknij **Czynności dot. replik**.
3. Kliknij **Przełączanie awaryjne**.
4. Wybierz, czy włączona replika ma zostać podłączona do sieci. Domyślnie replika zostanie podłączona do tej samej sieci co pierwotna maszyna.
5. [Opcjonalnie] Jeśli zdecydujesz się na podłączenie repliki do sieci, wyczyść zaznaczenie pola wyboru **Zatrzymaj oryginalną maszynę wirtualną**, aby utrzymać pierwotną maszynę w trybie online.
6. Kliknij **Rozpocznij**.

Gdy replika jest w stanie przełączania awaryjnego, możesz wybrać jedną z następujących czynności:

- **Zatrzymaj przełączanie awaryjne** (s. 129)

  Zatrzymaj przełączanie awaryjne, jeśli pierwotna maszyna została naprawiona. Replika zostanie wyłączona. Nastąpi wznowienie replikacji.
- **Wykonaj trwałe przełączenie awaryjne na replikę** (s. 129)

  Ta natychmiastowa operacja powoduje usunięcie flagi „replika” z maszyny wirtualnej, uniemożliwiając używanie tej maszyny jako lokalizacji docelowej replikacji. Jeśli zechcesz wznowić replikację, edytuj plan replikacji, wybierając tę maszynę jako źródło.
- **Powrót po awarii** (s. 129)

  W przypadku przełączenia awaryjnego na lokalizację, która nie jest przeznaczona do ciągłej obsługi operacji, wykonaj powrót po awarii. Replika zostanie odzyskana na pierwotną lub nową maszynę wirtualną. Po zakończeniu odzyskiwania na maszynę pierwotną maszyna ta zostanie włączona i nastąpi wznowienie replikacji. Jeśli zdecydujesz się na odzyskanie na nową maszynę, edytuj plan replikacji, wybierając tę maszynę jako źródło.

Copyright © Acronis International GmbH, 2002-2017

13.2.3.1 Zatrzymywanie przełączania awaryjnego

Aby zatrzymać przełączanie awaryjne

1. Wybierz replikę znajdującą się w stanie przełączania awaryjnego.
2. Kliknij **Czynności dot. replik**.
3. Kliknij **Zatrzymaj przełączanie awaryjne**.
4. Potwierdź decyzję.

13.2.3.2 Wykonywanie trwałego przełączenia awaryjnego

Aby wykonać trwałe przełączenie awaryjne

1. Wybierz replikę znajdującą się w stanie przełączania awaryjnego.
2. Kliknij **Czynności dot. replik**.
3. Kliknij **Trwałe przełączenie awaryjne**.
4. [Opcjonalnie] Zmień nazwę maszyny wirtualnej.
5. [Opcjonalnie] Zaznacz pole wyboru **Zatrzymaj oryginalną maszynę wirtualną**.
6. Kliknij **Rozpocznij**.

13.2.3.3 Wykonywanie powrotu po awarii

Aby wykonać operację powrotu po awarii z repliki

1. Wybierz replikę znajdującą się w stanie przełączania awaryjnego.
2. Kliknij **Czynności dot. replik**.
3. Kliknij **Powrót po awarii z repliki**.

   Program automatycznie wybierze pierwotny komputer jako komputer docelowy.
4. [Opcjonalnie] Kliknij **Komputer docelowy**, a następnie zrób tak:
   a. Określ, czy chcesz wykonać powrót po awarii na nową, czy na już istniejącą maszynę.
   b. Wybierz host ESXi i określ nazwę nowej maszyny lub wybierz maszynę już istniejącą.
   c. Kliknij **OK**.
5. [Opcjonalnie] W przypadku wykonywania powrotu po awarii na nową maszynę możesz też zrobić tak:
   - Kliknij **Magazyn danych**, aby wybrać magazyn danych dla maszyny wirtualnej.
   - Kliknij **Ustawienia maszyny wirtualnej**, aby zmienić rozmiar pamięci, liczbę procesorów oraz połączenia sieciowe maszyny wirtualnej.
6. [Opcjonalnie] Kliknij **Opcje odzyskiwania**, aby zmodyfikować opcje powrotu po awarii (s. 130).
7. Kliknij **Rozpocznij odzyskiwanie**.
8. Potwierdź decyzję.

13.2.4 Opcje replikacji

Aby zmodyfikować opcje replikacji, kliknij ikonę koła zębatego widoczną obok nazwy planu replikacji, a następnie kliknij **Opcje replikacji**.

CBT (Changed Block Tracking)

Ta opcja jest podobna do opcji tworzenia kopii zapasowych „Changed Block Tracking (CBT)” (s. 58).

Copyright © Acronis International GmbH, 2002-2017

Alokowanie dysków

Ta opcja umożliwia określenie ustawień alokowania dysków na potrzeby repliki.

Ustawienie wstępne: **Alokowanie elastyczne**.

Dostępne są następujące wartości: **Alokowanie elastyczne**, **Alokowanie nieelastyczne**, **Zachowaj pierwotne ustawienie**.

Obsługa błędów

Ta opcja jest podobna do opcji tworzenia kopii zapasowych „Obsługa błędów” (s. 59).

Polecenia poprzedzające/następujące

Ta opcja jest podobna do opcji tworzenia kopii zapasowych „Polecenia poprzedzające/następujące” (s. 65).

Usługa kopiowania woluminów w tle (VSS) dla maszyn wirtualnych

Ta opcja jest podobna do opcji tworzenia kopii zapasowych „Usługa kopiowania woluminów w tle (VSS) dla maszyn wirtualnych” (s. 72).

13.2.5 Opcje powrotu po awarii

Aby zmodyfikować opcje powrotu po awarii, kliknij **Opcje odzyskiwania** podczas konfigurowania powrotu po awarii.

Obsługa błędów

Ta opcja jest podobna do opcji odzyskiwania o tej samej nazwie: „Obsługa błędów” (s. 88).

Wydajność

Ta opcja jest podobna do opcji odzyskiwania o tej samej nazwie: „Wydajność” (s. 89).

Polecenia poprzedzające/następujące

Ta opcja jest podobna do opcji odzyskiwania o tej samej nazwie: „Polecenia poprzedzające/następujące” (s. 90).

Zarządzanie zasilaniem maszyn wirtualnych

Ta opcja jest podobna do opcji odzyskiwania o tej samej nazwie: „Zarządzanie zasilaniem maszyn wirtualnych” (s. 91).

13.2.6 Seeding repliki początkowej

Aby przyspieszyć replikację do lokalizacji zdalnej i zmniejszyć obciążenie przepustowości sieci, można przeprowadzić seeding repliki.

Ważne *Aby można było wykonać seeding repliki, na docelowym hoście ESXi musi działać agent dla VMware (urządzenie wirtualne).*

Aby przeprowadzić seeding repliki początkowej

1. Wykonaj jedną z następujących czynności:
   - Jeśli pierwotna maszyna wirtualna może zostać wyłączona, wyłącz ją i przejdź do kroku 4.

Copyright © Acronis International GmbH, 2002-2017

- Jeśli pierwotna maszyna wirtualna nie może zostać wyłączona, przejdź do następnego kroku.

2. Utwórz plan replikacji (s. 127).

   Podczas tworzenia planu w polu **Komputer docelowy** wybierz **Nowa replika** oraz host ESXi, na którym znajduje się maszyna pierwotna.
3. Uruchom plan raz.

   Replika zostanie utworzona na pierwotnej maszynie ESXi.
4. Wyeksportuj pliki maszyny wirtualnej (lub repliki) na zewnętrzny dysk twardy.
   a. Podłącz zewnętrzny dysk twardy do komputera z działającym klientem vSphere.
   b. Połącz klienta vSphere z pierwotną maszyną vCenter\ESXi.
   c. Wybierz nowo utworzoną replikę w obszarze inwentaryzacji.
   d. Kliknij **Plik** > **Eksportuj** > **Eksportuj szablon OVF**.
   e. W polu **Katalog** określ folder na zewnętrznym dysku twardym.
   f. Kliknij **OK**.
5. Prześlij dysk twardy do lokalizacji zdalnej.
6. Zaimportuj replikę na docelową maszynę ESXi.
   a. Podłącz zewnętrzny dysk twardy do komputera z działającym klientem vSphere.
   b. Połącz klienta vSphere z docelową maszyną vCenter\ESXi.
   c. Kliknij **Plik** > **Wdróż szablon OVF**.
   d. W polu **Wdróż z pliku lub adresu URL** określ szablon wyeksportowany w kroku 4.
   e. Wykonaj procedurę importu.
7. Edytuj plan replikacji utworzony w kroku 2. W polu **Komputer docelowy** wybierz **Istniejąca już replika**, a następnie wybierz zaimportowaną replikę.

W wyniku tych działań oprogramowanie będzie nadal aktualizować replikę. Wszystkie replikacje będą przyrostowe.

13.3 Zarządzanie środowiskami wirtualizacji

Środowiska vSphere i Hyper-V można oglądać w ich macierzystej postaci. Gdy zostanie zainstalowany i zarejestrowany odpowiedni agent, w obszarze **Urządzenia** pojawi się karta **VMware** lub **Hyper-V**.

Karta **VMware** umożliwia zmianę poświadczeń dostępu dla serwera vCenter lub autonomicznego hosta ESXi bez ponownej instalacji agenta.

Aby zmienić poświadczenia dostępu dla serwera vCenter lub hosta ESXi

1. W obszarze **Urządzenia** kliknij **VMware**.
2. Kliknij **Hosty i klastry**.
3. Na liście **Hosty i klastry** (z prawej strony drzewa **Hosty i klastry**) wybierz serwer vCenter lub autonomiczny host ESXi, który został określony podczas instalacji agenta dla VMware.
4. Kliknij **Przegląd**.
5. W obszarze **Poświadczenia** kliknij nazwę użytkownika.
6. Określ nowe poświadczenia dostępu i kliknij **OK**.

13.4 Migracja komputera

Migracji komputera można dokonać przez odzyskanie jego kopii zapasowej na innym komputerze niż komputer pierwotny.

Copyright © Acronis International GmbH, 2002-2017

W poniższej tabeli zestawiono dostępne opcje migracji.

Typ komputera w kopii zapasowej	Dostępne lokalizacje docelowe odzyskiwania		
	Komputer fizyczny	Maszyna wirtualna ESXi	Maszyna wirtualna Hyper-V
Komputer fizyczny	+	+	+
Maszyna wirtualna VMware ESXi	+	+	+
Maszyna wirtualna Hyper-V	+	+	+

Instrukcje przeprowadzania migracji można znaleźć w następujących sekcjach:

- Migracja komputera fizycznego na maszynę wirtualną (P2V): „Komputer fizyczny na maszynę wirtualną” (s. 75)
- Migracja maszyny wirtualnej na maszynę wirtualną (V2V): „Maszyna wirtualna” (s. 76)
- Migracja maszyny wirtualnej na komputer fizyczny (V2P): „Maszyna wirtualna” (s. 76) lub „Odzyskiwanie dysków przy użyciu nośnika startowego” (s. 78)

Choć migrację V2P można przeprowadzić w interfejsie internetowym, w określonych przypadkach zalecamy użycie nośnika startowego. Czasem można użyć nośnika w celu dokonania migracji do środowiska ESXi lub Hyper-V.

Nośnik umożliwia następujące działania:

- Wybranie pojedynczych dysków lub woluminów do odzyskania.
- Ręczne zamapowanie dysków z kopii zapasowej na dyski komputera docelowego.
- Odtworzenie woluminów logicznych (LVM) lub programowej macierzy RAID systemu Linux na komputerze docelowym.
- Udostępnienie sterowników do określonego sprzętu, co jest krytyczne z perspektywy możliwości uruchamiania systemu.

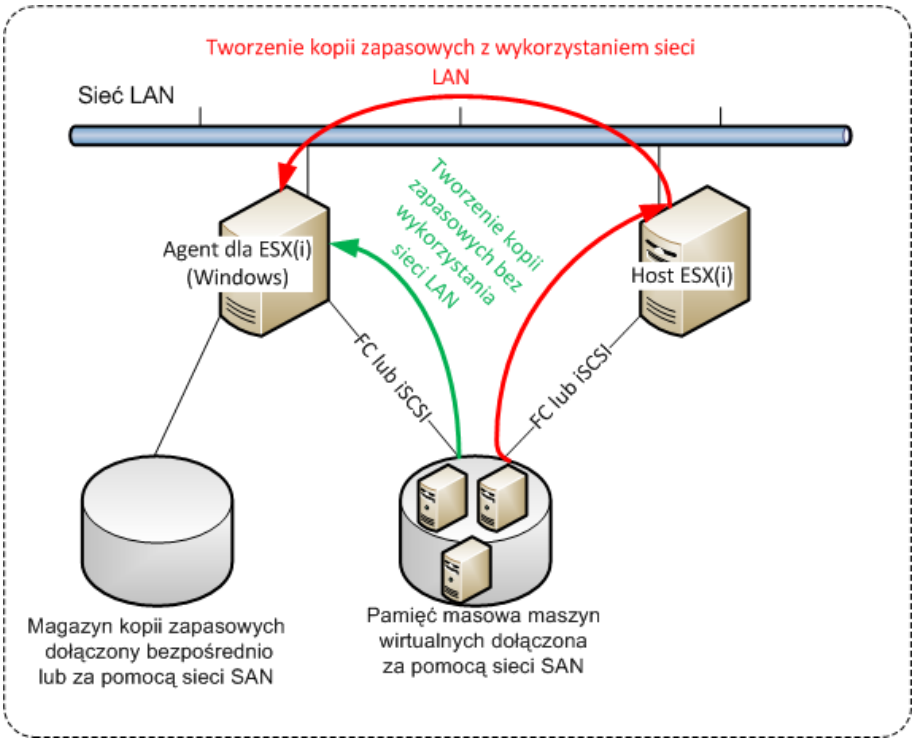
13.5 Agent dla VMware — tworzenie kopii zapasowych bez obciążania sieci lokalnej

Jeśli produkcyjne hosty ESXi są tak poważnie obciążone, że uruchamianie urządzeń wirtualnych jest niepożądane, rozważ instalację agenta dla VMware (Windows) na komputerze fizycznym znajdującym się poza infrastrukturą ESXi.

Jeśli system ESXi korzysta z pamięci masowej dołączonej do sieci SAN, zainstaluj agenta na komputerze podłączonym do tej samej sieci SAN. Agent będzie tworzył kopie zapasowe maszyn wirtualnych bezpośrednio z magazynu, a nie z hosta ESXi czy z sieci lokalnej. Funkcja ta jest nazywana tworzeniem kopii zapasowych bez obciążania sieci lokalnej.

Copyright © Acronis International GmbH, 2002-2017

Poniższa ilustracja przedstawia operację tworzenia kopii zapasowych opartego na sieci lokalnej oraz bez obciążania sieci lokalnej. Dostęp do maszyn wirtualnych z pominięciem sieci lokalnej jest możliwy w przypadku korzystania z łącza Fibre Channel (FC) lub sieci iSCSI Storage Area Network. Aby całkowicie wyeliminować konieczność przesyłania danych uwzględnianych w kopiach zapasowych przez sieć lokalną, przechowuj kopie zapasowe na dysku lokalnym komputera agenta lub na dołączonym magazynie SAN.



Aby umożliwić agentowi bezpośredni dostęp do magazynu danych

1. Zainstaluj agenta dla VMware na komputerze z systemem Windows, który ma dostęp przez sieć do serwera vCenter.
2. Podłącz do tego komputera jednostkę LUN zawierającą magazyn danych. Uwzględnij następujące wskazówki:
   - Użyj tego samego protokołu (np. iSCSI lub FC), którego używa połączenie magazynu danych z hostem ESXi.
   - *Nie wolno* zainicjować jednostki LUN i musi ona być widoczna w narzędziu **Zarządzanie dyskami** jako dysk „offline”. Jeśli system Windows zainicjuje jednostkę LUN, może ona ulec uszkodzeniu i środowisko VMware vSphere nie będzie mogło jej odczytać.

W związku z tym agent użyje trybu transportu SAN, aby uzyskać dostęp do dysków wirtualnych, tj. odczyta surowe sektory jednostki LUN przez interfejs iSCSI/FC bez rozpoznania systemu plików VMFS (o którym system Windows nie otrzymuje informacji).

Ograniczenia

- W środowisku vSphere w wersji 6.0 lub nowszej agent nie może korzystać z trybu transportu SAN, jeśli część dysków maszyny wirtualnej znajduje się na woluminie wirtualnym VMware Virtual Volume (VMware Virtual Volume — VVol), a część nie. Utworzenie kopii zapasowej takich maszyn wirtualnych się nie powiedzie.
- Kopie zapasowe szyfrowanych maszyn wirtualnych (takie maszyny wprowadzono w środowisku VMware vSphere 6.5) zostaną utworzone przy użyciu sieci lokalnej nawet w przypadku skonfigurowania dla agenta trybu transportu SAN. Ponieważ środowisko VMware nie obsługuje

Copyright © Acronis International GmbH, 2002-2017

tworzenia kopii zapasowych zaszyfrowanych dysków wirtualnych w trybie transportu SAN, agent wykona przełączenie awaryjne na tryb transportu NBD.

Przykład

Jeśli korzystasz z technologii iSCSI SAN, skonfiguruj inicjator iSCSI na komputerze z systemem Windows i zainstalowanym agentem dla VMware.

Aby zapobiec zainicjowaniu jednostki LUN, przed jej podłączeniem ustawimy **zasady SAN** na wartość **Współużytkowane offline**.

Aby skonfigurować zasady SAN

1. Zaloguj się jako administrator, otwórz wiersz polecenia, wpisz **`diskpart`** i naciśnij **Enter**.
2. Wpisz **`san policy=offlineshared`** i naciśnij **Enter**.
3. Aby sprawdzić, czy ustawienie zostało prawidłowo zastosowane, wpisz **`san`** i naciśnij **Enter**. Upewnij się, że jest wyświetlana opcja **Zasady SAN: Współużytkowane offline**.
4. Uruchom ponownie komputer.

Aby skonfigurować inicjator iSCSI

1. Przejdź do sekcji **Panel sterowania** > **Narzędzia administracyjne** > **Inicjator iSCSI**.

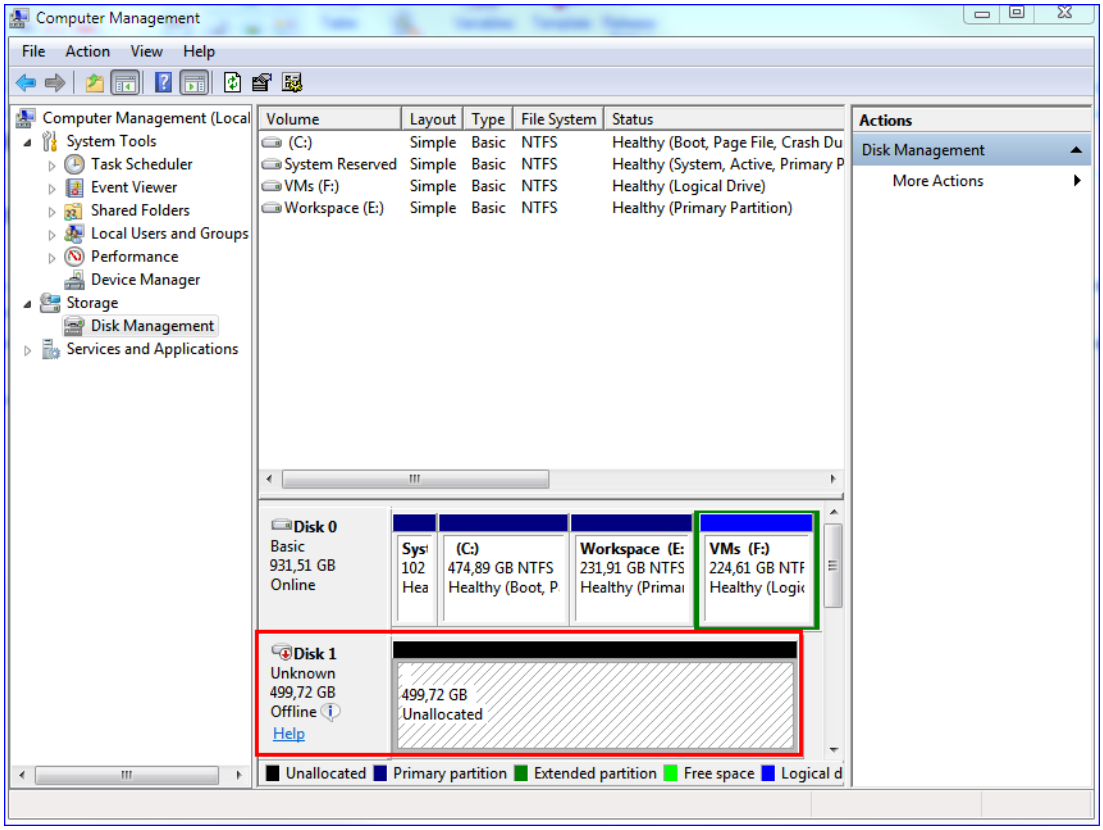
   Wskazówka. *Aby znaleźć aplet **Narzędzia administracyjne**, być może trzeba będzie zmienić widok w **Panelu sterowania** na inny niż **Narzędzia główne** czy **Kategoria** albo skorzystać z funkcji wyszukiwania.*

2. Jeśli inicjator Microsoft iSCSI jest uruchamiany po raz pierwszy, potwierdź, że chcesz uruchomić usługę inicjatora iSCSI firmy Microsoft.
3. Na karcie **Miejsca docelowe** wpisz w pełni kwalifikowaną nazwę domeny (FQDN) lub adres IP docelowego urządzenia SAN, a następnie kliknij **Quick Connect**.
4. Wybierz jednostkę LUN, na której znajduje się magazyn danych, a następnie kliknij **Połącz**.

   Jeśli jednostka LUN nie jest wyświetlana, upewnij się, że podział na strefy obiektu docelowego iSCSI umożliwia komputerowi z uruchomionym agentem dostęp o tej jednostki LUN. Komputer musi zostać dodany do listy dozwolonych inicjatorów iSCSI na tym obiekcie docelowym.
5. Kliknij **OK**.

Copyright © Acronis International GmbH, 2002-2017

Gotowa jednostka LUN sieci SAN powinna się pojawić w obszarze **Zarządzanie dyskami**, tak jak pokazano na poniższym zarzucie ekranu.



13.6 Agent dla VMware — niezbędne uprawnienia

W tej sekcji opisano uprawnienia wymagane do wykonywania operacji z udziałem maszyn wirtualnych ESXi, a także do wdrażania urządzeń wirtualnych. Agent dla VMware (urządzenie wirtualne) jest dostępny tylko w ramach wdrożenia lokalnego.

Aby wykonać operacje na wszystkich hostach i klastrach zarządzanych przez dany serwer vCenter, agent dla VMware musi mieć uprawnienia na tym serwerze. Jeśli działanie agenta ma się ograniczyć tylko do konkretnego hosta ESXi, należy agentowi przyznać te same uprawnienia na hoście.

Określ konto z niezbędnymi uprawnieniami podczas instalacji i konfiguracji agenta dla VMware. W razie późniejszej konieczności zmiany konta zajrzyj do sekcji „Zarządzanie środowiskami wirtualizacji” (s. 131).

		Operacja				
Obiekt	**Uprawnienie**	**Utworzenie kopii zapasowej maszyny wirtualnej**	**Odzyskanie na nową maszynę wirtualną**	**Odzyskanie na istniejącą maszynę wirtualną**	**Uruchom maszynę wirtualną z kopii zapasowej**	**Wdrożenie urządzenia wirtualnego**
Operacje kryptograficzne (począwszy od vSphere 6.5)	**Dodaj dysk**	+*				
	Dostęp bezpośredni	+*				

Copyright © Acronis International GmbH, 2002-2017

		Operacja				
Obiekt	**Uprawnienie**	**Utworzenie kopii zapasowej maszyny wirtualnej**	**Odzyskanie na nową maszynę wirtualną**	**Odzyskanie na istniejącą maszynę wirtualną**	**Uruchom maszynę wirtualną z kopii zapasowej**	**Wdrożenie urządzenia wirtualnego**
Magazyn danych	**Przydzielenie miejsca**		+	+	+	+
	Przeglądanie magazynu danych				+	+
	Konfigurowanie magazynu danych	+	+	+	+	+
	Niskopoziomowe operacje na plikach				+	+
Globalne	**Licencje**	+	+	+	+	
	Metody wyłączania	+	+	+		
	Metody włączania	+	+	+		
Host > **Konfiguracja**	**Konfiguracja automatycznego uruchamiania maszyny wirtualnej**					+
	Konfiguracja partycji magazynu				+	
Host > **Inwentaryzacja**	**Modyfikowanie klastra**					+
Host > **Operacje lokalne**	**Tworzenie maszyny wirtualnej**				+	+
	Usuwanie maszyny wirtualnej				+	+
	Ponowne konfigurowanie maszyny wirtualnej				+	+
Sieć	**Przypisanie sieci**		+	+	+	+
Zasób	**Przypisanie maszyny wirtualnej do puli zasobów**		+	+	+	+
vApp	**Importuj**					+
Maszyna wirtualna > **Konfiguracja**	**Dodanie istniejącego dysku**	+	+		+	
	Dodaj nowy dysk		+	+	+	+
	Dodanie lub usunięcie urządzenia		+		+	+

Copyright © Acronis International GmbH, 2002-2017

		Operacja				
Obiekt	**Uprawnienie**	**Utworzenie kopii zapasowej maszyny wirtualnej**	**Odzyskanie na nową maszynę wirtualną**	**Odzyskanie na istniejącą maszynę wirtualną**	**Uruchom maszynę wirtualną z kopii zapasowej**	**Wdrożenie urządzenia wirtualnego**
	Zaawansowany	+	+	+		+
	Zmiana liczby procesorów		+			
	Śledzenie zmian na dysku	+		+		
	Dzierżawa dysku	+		+		
	Pamięć		+			
	Usunięcie dysku	+	+	+	+	
	Zmień nazwę		+			
	Ustaw adnotację				+	
	Ustawienia		+	+		
Maszyna wirtualna > Operacje gościa	**Wykonanie programu operacji gościa**	+**				+
	Zapytania operacji gościa	+**				+
Maszyna wirtualna > Interakcja	**Uzyskaj bilet kontroli gościa** (w środowisku vSphere 4.1 i 5.0)				+	+
	Konfiguracja nośnika CD		+	+		
	Interakcja z konsolą					+
	Zarządzanie systemem operacyjnym-gościem za pośrednictwem interfejsu API VIX (w środowisku vSphere w wersji 5.1 lub nowszej)				+	+
	Wyłączenie zasilania			+	+	+
	Włączenie zasilania		+	+	+	+
Maszyna wirtualna > Inwentaryzacja	**Utworzenie na podstawie istniejącej**		+	+	+	
	Utwórz nowy		+	+	+	+
	Przenieś					+
	Rejestruj				+	

Copyright © Acronis International GmbH, 2002-2017

		Operacja				
Obiekt	**Uprawnienie**	**Utworzenie kopii zapasowej maszyny wirtualnej**	**Odzyskanie na nową maszynę wirtualną**	**Odzyskanie na istniejącą maszynę wirtualną**	**Uruchom maszynę wirtualną z kopii zapasowej**	**Wdrożenie urządzenia wirtualnego**
	Usuń		+	+	+	+
	Wyrejestruj				+	
Maszyna wirtualna > Alokowanie	**Zezwolenie na dostęp do dysku**		+	+	+	
	Zezwól na dostęp do dysku w trybie tylko do odczytu	+		+		
	Zezwolenie na pobranie maszyny wirtualnej	+	+	+	+	
Maszyna wirtualna > Stan	**Utworzenie migawki**	+		+	+	+
	Usunięcie migawki	+		+	+	+

* To uprawnienie jest wymagane tylko w przypadku tworzenia kopii zapasowej zaszyfrowanych komputerów.

** To uprawnienie jest wymagane tylko w przypadku kopii zapasowych uwzględniających aplikacje.

13.7 Maszyny wirtualne Windows Azure i Amazon EC2

Aby utworzyć kopię zapasową maszyny wirtualnej Windows Azure lub Amazon EC2, zainstaluj na tej maszynie agenta kopii zapasowych. Tworzenie kopii zapasowych i odzyskiwanie przebiega identycznie jak w przypadku komputera fizycznego. Niemniej jednak w przypadku ustawienia limitów liczby komputerów we wdrożeniu chmurowym komputer jest traktowany jako maszyna wirtualna.

Różnica w porównaniu z komputerem fizycznym polega na tym, że maszyn wirtualnych Windows Azure i Amazon EC2 nie można uruchamiać z nośnika startowego. Jeśli zajdzie potrzeba odzyskania na nową maszynę wirtualną Windows Azure lub Amazon EC2, wykonaj poniższą procedurę.

Aby odzyskać komputer jako maszynę wirtualną Windows Azure lub Amazon EC2

1. Utwórz nową maszynę wirtualną z obrazu/szablonu w środowisku Windows Azure lub Amazon EC2. Nowa maszyna musi mieć taką samą konfigurację dysków jak odzyskiwany komputer.
2. Zainstaluj na nowej maszynie wirtualnej agenta dla systemu Windows lub agenta dla systemu Linux.
3. Odzyskaj komputer z kopii zapasowej zgodnie z opisem zamieszczonym w sekcji „Komputer fizyczny” (s. 74). Konfigurując odzyskiwanie, wybierz nową maszynę jako komputer docelowy.

Wymagania dotyczące sieci

Agenty zainstalowane na komputerach uwzględnianych w kopiach zapasowych muszą mieć możliwość komunikowania się przez sieć z serwerem zarządzania.

Wdrożenie lokalne

- Jeśli zarówno agenty, jak i serwer zarządzania są zainstalowane w chmurze Azure/EC2, wszystkie komputery już się znajdują w tej samej sieci. Nie trzeba wykonywać dodatkowych czynności.

Copyright © Acronis International GmbH, 2002-2017

- Jeśli serwer zarządzania znajduje się poza chmurą Azure/EC2, komputery w chmurze nie będą mieć dostępu sieciowego do sieci lokalnej, w której jest zainstalowany serwer zarządzania. Aby umożliwić agentom zainstalowanym na takich komputerach komunikację z serwerem zarządzania, trzeba utworzyć połączenie VPN między siecią lokalną (w firmie) a chmurą (Azure/EC2). Instrukcje tworzenia połączenia VPN można znaleźć w następujących artykułach:

  Amazon EC2:
  http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_VPN.html#vpn-create-cgw

  Windows Azure:
  https://azure.microsoft.com/pl-pl/documentation/articles/vpn-gateway-site-to-site-create

Wdrożenie chmurowe

We wdrożeniu chmurowym serwer zarządzania znajduje się w jednym z centrów danych Acronis i w związku z tym jest dostępny dla agentów. Nie trzeba wykonywać dodatkowych czynności.

14 Ustawienia serwera zarządzania

Ustawienia te są dostępne tylko w ramach wdrożeń lokalnych.

Aby uzyskać do nich dostęp, kliknij **Ustawienia** > **Ustawienia systemowe**.

Aby uzyskać informacje na temat zarządzania licencjami programu Acronis Backup, zobacz sekcję „Zarządzanie licencjami” (s. 31).

14.1 Serwer e-mail

Można określić serwer poczty e-mail, który będzie używany do wysyłania powiadomień e-mail z serwera zarządzania.

Aby określić serwer poczty e-mail

1. Kliknij **Ustawienia** > **Ustawienia systemowe** > **Serwer e-mail**.
2. W polu **Szyfrowanie** wybierz jedno z następujących ustawień:
   - **Niestandardowe**
   - **Gmail**

     Na koncie Gmail musi być włączona opcja **Mniej bezpieczne aplikacje**. Aby uzyskać więcej informacji, zobacz https://support.google.com/accounts/answer/6010255.
   - **Yahoo Mail**
   - **Outlook.com**
3. [Tylko w przypadku niestandardowej usługi poczty e-mail] Określ następujące ustawienia:
   - W polu **Serwer SMTP** wprowadź nazwę serwera poczty wychodzącej (SMTP).
   - W polu **Port SMTP** ustaw port serwera poczty wychodzącej. Domyślnie jest to port 25.
   - Wybierz, czy chcesz stosować szyfrowanie SSL, czy TLS. Wybierz **Brak**, aby wyłączyć szyfrowanie.
   - Jeśli serwer SMTP wymaga uwierzytelnienia, zaznacz pole wyboru **Serwer SMTP wymaga uwierzytelnienia**, a następnie określ poświadczenia konta, które będzie używane do wysyłania wiadomości. Jeśli nie wiesz, czy serwer SMTP wymaga uwierzytelnienia, skontaktuj się z administratorem sieci lub dostawcą usług poczty e-mail w celu uzyskania pomocy.
   - Niektórzy dostawcy usług internetowych umożliwiają wysłanie poczty dopiero po uwierzytelnieniu na serwerze poczty przychodzącej. Jeśli tak jest, zaznacz pole wyboru

Copyright © Acronis International GmbH, 2002-2017

Skonfiguruj serwer poczty przychodzącej (POP), aby włączyć serwer POP i skonfigurować jego ustawienia:

- W polu **Serwer POP** wprowadź nazwę serwera POP.
- W polu **Port POP** ustaw port serwera poczty przychodzącej. Domyślnie jest to port 110.
- Określ poświadczenia dostępu dla serwera poczty przychodzącej.

4. [Tylko w przypadku usług Gmail, Yahoo Mail i Outlook.com] Określ poświadczenia konta, które będzie używane do wysyłania wiadomości.
5. W polu **Nadawca** wpisz imię i nazwisko nadawcy. Wprowadzone imię i nazwisko będą wyświetlane w polu **Od** w powiadomieniach e-mail. Jeśli to pole pozostanie puste, wiadomości będą zawierały konto określone w kroku 3 lub 4.
6. [Opcjonalnie] Kliknij **Wyślij wiadomość próbną**, aby sprawdzić, czy powiadomienia e-mail działają prawidłowo przy określonych ustawieniach. Wprowadź adres e-mail, na który ma zostać wysłana wiadomość próbna.

14.2 Powiadomienia e-mail

Istnieje możliwość skonfigurowania ustawień domyślnych wszystkich powiadomień e-mail wysyłanych z serwera zarządzania.

Podczas tworzenia planu tworzenia kopii zapasowych można użyć ustawień domyślnych lub zastąpić je wartościami niestandardowymi, które będą stosowane tylko w odniesieniu do tego planu.

Ważne *Zmiana ustawień domyślnych wpłynie na wszystkie korzystające z nich plany tworzenia kopii zapasowych.*

Zanim skonfigurujesz te ustawienia, upewnij się, że zostały skonfigurowane ustawienia **serwera poczty e-mail** (s. 139).

Aby skonfigurować domyślne ustawienia powiadomień e-mail

1. Kliknij **Ustawienia** > **Ustawienia systemowe** > **Powiadomienia e-mail**.
2. W polu **Adresy e-mail odbiorców** wpisz docelowy adres e-mail. Możesz wprowadzić kilka adresów oddzielonych średnikami.
3. Wybierz typy powiadomień, które mają być wysyłane. Dostępne są następujące typy:
   - **Błędy**
   - **Ostrzeżenia**
   - **Udane kopie zapasowe**

Temat wiadomości e-mail ma następującą strukturę: **[temat] [nazwa komputera] [nazwa planu tworzenia kopii zapasowych]**. Zmienna **[temat]** jest zastępowana jednym z następujących tekstów: **Pomyślnie utworzono kopię zapasową**, **Utworzenie kopii zapasowej nie powiodło się**, **Kopia zapasowa została utworzona z ostrzeżeniami**.

15 Zarządzanie grupami i kontami

Funkcje opisane w tej sekcji są dostępne tylko w ramach wdrożenia chmurowego w przypadku kont z uprawnieniami administracyjnymi.

Copyright © Acronis International GmbH, 2002-2017

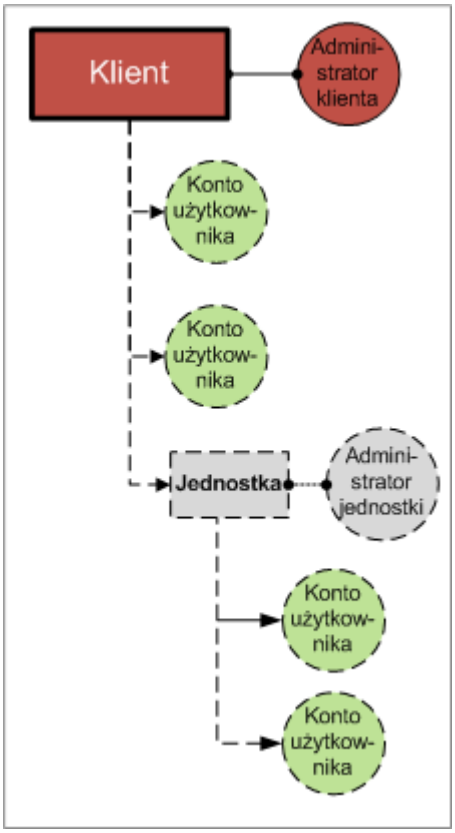
15.1 Konta i grupy

Dostępne są dwa rodzaje kont: **konta administratorów** oraz **konta użytkowników**. Zarówno użytkownik, jak i administratorzy mogą zarządzać kopiami zapasowymi danych użytkownika.

Każde konto należy do jakiejś grupy. Grupa **Klient** jest tworzona automatycznie dla danej organizacji. Opcjonalnie można utworzyć grupy **Jednostka**, które zwykle odpowiadają jednostkom organizacyjnym lub działom organizacji.

Administrator może tworzyć grupy, konta administratorów i konta użytkowników oraz zarządzać nimi — na własnym lub niższym poziomie hierarchii.

Poniższy diagram ilustruje dwa poziomy hierarchii — grupę klienta i grupy jednostek. Opcjonalne grupy i konta są oznaczone linią kropkowaną.



Poniższa tabela zawiera zestawienie operacji, które mogą wykonywać administratorzy oraz użytkownicy.

Operacja	Użytkownicy	Administratorzy
Tworzenie grup	Nie	Tak
Tworzenie kont	Nie	Tak
Pobieranie i instalacja oprogramowania do tworzenia kopii zapasowych	Tak	Tak
Zarządzanie kopiami zapasowymi	Tak	Tak
Zarządzanie odzyskiwaniem	Tak	Tak

Copyright © Acronis International GmbH, 2002-2017

Tworzenie raportów dotyczących użytkowania usługi	Nie	Tak

15.2 Tworzenie grupy

W przypadku objęcia usługą tworzenia kopii zapasowych nowej jednostki organizacyjnej można utworzyć w firmie nową grupę **Jednostka**.

Aby utworzyć grupę

1. Zaloguj się do konsoli kopii zapasowych.
2. Kliknij **Zarządzaj kontami**.
3. Wybierz grupę, w której chcesz utworzyć nową grupę.
4. U dołu panelu **Grupy** kliknij „**+**”.
5. W polu **Nazwa** określ nazwę nowej grupy.
6. [Opcjonalnie] W polu **Identyfikator** wpisz ciąg, który będzie służyć jako identyfikator grupy. Identyfikator ten będzie widoczny w raportach miesięcznych wraz z danymi dotyczącymi użytkowania usługi w ramach grupy. Może on służyć do odwoływania się do grupy w innym oprogramowaniu, np. w systemach rozliczeń i monitorowania.

   Identyfikator może się składać z maksymalnie 256 znaków Unicode (na przykład cyfr oraz liter alfabetu łacińskiego). Nie musi on być unikatowy dla danej grupy.
7. W polu **Język domyślny** wybierz domyślny język powiadomień, raportów i oprogramowania do tworzenia kopii zapasowych. Będzie on używany w obrębie grupy.
8. [Opcjonalnie] W polu **Lokalizacje kopii zapasowych** wybierz lokalizacje kopii zapasowych dla grupy i jej grup podrzędnych. Dostępne są następujące wartości:
   - **Lokalnie i chmura**
   - **Tylko chmura**
9. [Opcjonalnie] Wyłącz przełącznik **Automatyczna aktualizacja agenta**. Jeśli to zrobisz, agenty zarejestrowane na kontach w tej grupie i jej grupach podrzędnych nie będą aktualizowane automatycznie po wydaniu nowej wersji.
10. [Opcjonalnie] W polu **Informacje kontaktowe** określ informacje kontaktowe dotyczące grupy.
11. Kliknij **Utwórz**.

W drzewie **Grupy** pojawi się nowo utworzona grupa.

Aby określić informacje rozliczeniowe dotyczące grupy, wybierz grupę z listy **Grupy**, kliknij **Właściwości** i wypełnij sekcję informacji rozliczeniowych.

15.3 Tworzenie konta

W ramach jednostki musi istnieć co najmniej jedno konto (administratora lub użytkownika).

Aby utworzyć konto

1. Zaloguj się do konsoli kopii zapasowych.
2. Kliknij **Zarządzaj kontami**.
3. Wybierz grupę, w której chcesz utworzyć konto.
4. Kliknij kartę **Konta**.
5. Kliknij **Dodaj konto**.
6. Określ następujące informacje kontaktowe na potrzeby konta.

Copyright © Acronis International GmbH, 2002-2017

- **Nazwa logowania**

  Ważne *Każde konto musi mieć unikatową nazwę logowania. Przy użyciu jednego adresu e-mail można utworzyć wiele nazw logowania.*

- **Adres e-mail**
- [Opcjonalnie]**Imię**
- [Opcjonalnie] **Nazwisko**

7. Jeśli ma to być konto administratora, włącz przełącznik **Uprawnienia administratora**.
8. [Opcjonalnie] Wyłącz przełącznik **Automatyczna aktualizacja agenta**. Jeśli to zrobisz, agenty zarejestrowane na tym koncie nie będą aktualizowane automatycznie po wydaniu nowej wersji.
9. [Opcjonalnie] Określ limit miejsca oraz maksymalną liczbę komputerów / urządzeń / skrzynek pocztowych, które użytkownik może uwzględnić w kopii zapasowej.
   - **Fizyczne stacje robocze**
   - **Serwery fizyczne**
   - **Windows Server Essentials**
   - **Hosty wirtualne**
   - **Urządzenia mobilne**
   - **Skrzynki pocztowe Office 365**
   - **Limit miejsca**

   Limity są elastyczne. Jeśli którakolwiek z tych wartości zostanie przekroczona, na adres e-mail określony w kroku 6 zostanie wysłane powiadomienie. Ograniczenia dotyczące korzystania z usługi kopii zapasowych nie są stosowane.
10. [Opcjonalnie] Określ nadwyżki limitów. Nadwyżka umożliwia użytkownikowi przekroczenie limitu o określoną wartość. W przypadku przekroczenia nadwyżki tworzenie kopii zapasowej zakończy się niepowodzeniem.

    Ważne *Jeśli zarówno limit, jak i nadwyżka będą mieć wartość zero, związane z nimi funkcje zostaną ukryte przed użytkownikiem.*

11. [Opcjonalnie] W polu **Lokalizacje kopii zapasowych** wybierz lokalizacje kopii zapasowych dla tego konta. Dostępne są następujące wartości:
    - **Lokalnie i chmura**
    - **Tylko chmura**
12. [Opcjonalnie] Zmień poziom w polu **Powiadomienia dotyczące kopii zapasowych**. Możesz wybrać jeden z następujących poziomów:
    - **Wyłączone**. Brak powiadomień
    - **Mniej**: Powiadomienia o niepowodzeniu tworzenia kopii zapasowej (domyślne)
    - **Więcej**: Powiadomienia o niepowodzeniu tworzenia kopii zapasowej i ostrzeżenia (domyślne)
    - **Wszystkie**: Powiadomienia o niepowodzeniu tworzenia kopii zapasowej i o pomyślnym jej utworzeniu oraz ostrzeżenia

    Wszystkie powiadomienia będą wysyłane na podany adres e-mail.
13. [Opcjonalnie] Wyłącz **Powiadomienia biznesowe**. Jeśli to zrobisz, powiadomienia o przekroczonych limitach nie będą wysyłane na określony adres e-mail.
14. Kliknij **Dodaj**.

Wskutek tego:

- Na karcie **Konta** pojawi się nowe konto.

Copyright © Acronis International GmbH, 2002-2017

- Na określony adres e-mail zostanie wysłana wiadomość e-mail zawierająca łącze aktywacji.

15.4 Tworzenie raportu dotyczącego użytkowania usługi

Raporty z użytkowania zawierają dane historyczne o korzystaniu z usługi kopii zapasowych.

Raporty te mogą tworzyć tylko administratorzy.

Parametry raportu

Raport zawiera następujące dane dotyczące jednostki i jej kont:

- Rozmiar kopii zapasowych według grupy, konta i typu komputera.
- Liczba chronionych komputerów według grupy, konta i typu komputera.
- Wartość cenowa według grupy, konta i typu komputera.
- Łączny rozmiar kopii zapasowych.
- Łączna liczba chronionych komputerów.
- Łączna wartość cenowa.

Zakres raportu

W razie potrzeby można wskazać zakres raportu, wybierając jedną z poniższych wartości:

- **Bezpośredni klienci i partnerzy**

  Raport będzie zawierać tylko wartości parametrów raportu dotyczące bezpośrednich grup podrzędnych danej grupy.
- **Wszyscy klienci i partnerzy**

  Raport będzie zawierać wartości parametrów raportu dotyczące wszystkich grup podrzędnych danej grupy.
- **Wszyscy klienci i partnerzy (w tym szczegółowe dane konta)**

  Raport będzie zawierać wartości parametrów raportu dotyczące wszystkich grup podrzędnych danej grupy oraz wszystkich kont użytkowników w tych grupach.

Włączanie lub wyłączanie zaplanowanych raportów z użytkowania

Zaplanowany raport obejmuje dane dotyczące wykorzystania systemu w ostatnim pełnym miesiącu kalendarzowym. Raporty są generowane pierwszego dnia miesiąca o godzinie 23:59:59 czasu UTC i wysyłane na drugi dzień do wszystkich administratorów grupy.

1. W konsoli zarządzania kontami kliknij **Raporty**.
2. Wybierz **Zaplanowane**.
3. Włącz lub wyłącz zaplanowane raporty z użytkowania, klikając Włącz/Wyłącz.
4. W polu **Poziom szczegółów** wybierz zakres raportu zgodnie z wcześniejszym opisem.

Generowanie niestandardowego raportu z użytkowania

Tego typu raport można wygenerować na żądanie — nie można go zaplanować. Raport zostanie wysłany na Twój adres e-mail.

1. W konsoli zarządzania kontami kliknij **Raporty**.
2. Wybierz kartę **Niestandardowe**.
3. W polu **Okres** wybierz okres raportowania:
   - **Obecny miesiąc kalendarzowy**
   - **Poprzedni miesiąc kalendarzowy**

Copyright © Acronis International GmbH, 2002-2017

- **Niestandardowe**

4. Jeśli chcesz wskazać niestandardowy okres raportowania, wybierz datę początkową i końcową. W przeciwnym razie pomiń ten krok.
5. W polu **Typ** wybierz typ raportu:
   - **Raport podsumowujący** — raport będzie obejmować łączne wartości parametrów raportu dla wskazanego okresu, w tym łączną wartość cenową.
   - **Statystyka dzienna** — raport będzie obejmować wartości parametrów raportu dla poszczególnych dni we wskazanym okresie, bez wartości cenowych.
6. W polu **Poziom szczegółów** wybierz zakres raportu zgodnie z wcześniejszym opisem.
7. Aby wygenerować raport, kliknij **Wygeneruj i wyślij**.

15.5 Ograniczanie dostępu do interfejsu internetowego

Dostęp do interfejsu internetowego można ograniczyć, określając listę adresów IP, z których mogą się logować członkowie grupy.

Takie ograniczenie *nie* jest stosowane w przypadku członków grup podrzędnych.

Aby ograniczyć dostęp do interfejsu internetowego

1. Zaloguj się do konsoli zarządzania kontami.
2. Wybierz grupę, w której przypadku chcesz ograniczyć dostęp.
3. Kliknij **Ustawienia** > **Zabezpieczenia**.
4. Zaznacz pole wyboru **Włącz kontrolę logowania**.
5. W polu **Dozwolone adresy IP** określ dozwolone adresy IP.

   Możesz wprowadzić dowolne z poniższych parametrów, oddzielając je średnikiem:
   - Adresy IP, na przykład 192.0.2.0
   - Zakresy adresów IP, na przykład 192.0.2.0-192.0.2.255
   - Podsieci, na przykład 192.0.2.0/24
6. Kliknij **Zapisz**.

16 Rozwiązywanie problemów

W tej sekcji opisano, jak zapisać dziennik agenta w pliku ZIP. Jeśli operacja tworzenia kopii zapasowej nie powiedzie się z nieznanych przyczyn, plik ten pomoże pracownikom pomocy technicznej w zdiagnozowaniu problemu.

Aby zebrać dzienniki

1. Wybierz komputer, z którego chcesz zebrać dzienniki.
2. Kliknij **Działania**.
3. Kliknij **Zbierz informacje o systemie**.
4. Jeśli przeglądarka wyświetli monit, określ, gdzie ma zostać zapisany plik.

Copyright © Acronis International GmbH, 2002-2017

Oświadczenie dotyczące praw autorskich

Copyright © Acronis International GmbH, 2002-2017. Wszelkie prawa zastrzeżone.

„Acronis” i „Acronis Secure Zone” są zastrzeżonymi znakami towarowymi firmy Acronis International GmbH.

„Acronis Compute with Confidence”, „Acronis Startup Recovery Manager”, „Acronis Active Restore”, „Acronis Instant Restore” i logo Acronis są znakami towarowymi firmy Acronis International GmbH.

Linux jest zastrzeżonym znakiem towarowym Linusa Torvaldsa.

VMware i VMware Ready są znakami towarowymi lub zastrzeżonymi znakami towarowymi VMware, Inc. w Stanach Zjednoczonych i/lub innych jurysdykcjach.

Windows i MS-DOS są zastrzeżonymi znakami towarowymi firmy Microsoft Corporation.

Wszystkie inne wymienione znaki towarowe i prawa autorskie stanowią własność ich odpowiednich właścicieli.

Rozpowszechnianie niniejszego dokumentu w wersjach znacząco zmienionych jest zabronione bez wyraźnej zgody właściciela praw autorskich.

Rozpowszechnianie niniejszego lub podobnego opracowania w jakiejkolwiek postaci książkowej (papierowej) dla celów handlowych jest zabronione bez uprzedniej zgody właściciela praw autorskich.

DOKUMENTACJA ZOSTAJE DOSTARCZONA W TAKIM STANIE, W JAKIM JEST („TAK JAK JEST”) I WSZYSTKIE WARUNKI, OŚWIADCZENIA I DEKLARACJE WYRAŹNE LUB DOROZUMIANE, W TYM WSZELKIE GWARANCJE ZBYWALNOŚCI, PRZYDATNOŚCI DO OKREŚLONEGO CELU LUB NIENARUSZANIA PRAW ZOSTAJĄ WYŁĄCZONE, Z WYJĄTKIEM ZAKRESU, W JAKIM TE WYŁĄCZENIA ZOSTANĄ UZNANE ZA NIEZGODNE Z PRAWEM.

Oprogramowanie i/lub Usługa mogą zawierać kod innych firm. Warunki licencji takich producentów zawarte są w pliku license.txt znajdującym się w głównym katalogu instalacyjnym. Najnowsze informacje dotyczące kodu innych firm zawartego w Oprogramowaniu i/lub Usłudze oraz związane z nimi warunki licencji można znaleźć pod adresem http://kb.acronis.com/content/7696.

Opatentowane technologie firmy Acronis

Technologie zastosowane w tym produkcie są objęte i chronione jednym lub wieloma spośród następujących patentów przyznanych w USA: 7,047,380; 7,275,139; 7,281,104; 7,318,135; 7,353,355; 7,366,859; 7,475,282; 7,603,533; 7,636,824; 7,650,473; 7,721,138; 7,779,221; 7,831,789; 7,886,120; 7,895,403; 7,934,064; 7,937,612; 7,949,635; 7,953,948; 7,979,690; 8,005,797; 8,051,044; 8,069,320; 8,073,815; 8,074,035; 8,145,607; 8,180,984; 8,225,133; 8,261,035; 8,296,264; 8,312,259; 8,347,137; 8,484,427; 8,645,748; 8,732,121; zgłoszono również wnioski patentowe oczekujące na rozpatrzenie.

17 Słownik

F

Format jednoplikowej kopii zapasowej

Nowy format kopii zapasowych, w którym początkowa pełna kopia zapasowa i późniejsze przyrostowe kopie zapasowe są zapisywane w jednym pliku .tib, a nie w ciągu plików. W formacie tym wykorzystano szybkość metody tworzenia przyrostowych kopii zapasowych, unikając najpoważniejszej wady tej metody — trudności związanych z usuwaniem przestarzałych kopii zapasowych. Oprogramowanie oznacza bloki zajmowane przez przestarzałe kopie zapasowe jako „wolne” i korzysta z nich podczas zapisywania nowych kopii zapasowych. Umożliwia to nadzwyczaj szybkie czyszczenie przy minimalnym obciążeniu zasobów.

Format jednoplikowej kopii zapasowej jest niedostępny w przypadku tworzenia kopii zapasowej w lokalizacji nieobsługującej operacji odczytu i zapisu w dostępie losowym.

P

Pełna kopia zapasowa

Samowystarczalna kopia zapasowa zawierająca wszystkie dane wybrane do uwzględnienia w kopii zapasowej. Aby odzyskać dane z pełnej kopii zapasowej, nie trzeba korzystać z żadnej innej kopii.

Przyrostowa kopia zapasowa

Kopia zapasowa, która zapisuje dane zmienione względem najnowszej kopii zapasowej. Aby odzyskać dane z przyrostowej kopii zapasowej, potrzebny jest dostęp do innych kopii zapasowych.

R

Różnicowa kopia zapasowa

Różnicowa kopia zapasowa zapisuje dane zmienione względem najnowszej pełnej kopii zapasowej (s. 147). Aby odzyskać dane z różnicowej kopii zapasowej, należy uzyskać dostęp do odpowiedniej pełnej kopii zapasowej.

Z

Zestaw kopii zapasowych

Grupa kopii zapasowych, do których można zastosować odrębną regułę przechowywania.

W przypadku schematu tworzenia kopii zapasowych **Niestandardowy** zestawy kopii zapasowych odpowiadają metodom tworzenia kopii zapasowych (**Pełna**, **Różnicowa** i **Przyrostowa**).

W innych przypadkach zestawami kopii zapasowych są grupy **Co miesiąc**, **Codziennie**, **Co tydzień** oraz **Co godzinę**.

- Miesięczną kopią zapasową jest pierwsza kopia zapasowa utworzona po rozpoczęciu miesiąca.

Copyright © Acronis International GmbH, 2002-2017

- Tygodniową kopią zapasową jest pierwsza kopia zapasowa utworzona w dniu tygodnia wybranym w polu **Tygodniowa kopia zapasowa** (kliknij ikonę koła zębatego, a następnie **Opcje tworzenia kopii zapasowych** > **Tygodniowa kopia zapasowy**).
- Dzienną kopią zapasową jest pierwsza kopia zapasowa utworzona po rozpoczęciu dnia.
- Godzinną kopią zapasową jest pierwsza kopia zapasowa utworzona po rozpoczęciu godziny.

Copyright © Acronis International GmbH, 2002-2017