Acronis

acronis.com

Acronis Cyber Protect 15

Update 6

Podręcznik użytkownika

WERSJA: 15.06.2023

Spis treści

Oświadczenie dotyczące praw autorskich

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; 7,246,211; 7,275,139; 7,281,104; 7,318,135; 7,353,355; 7,366,859; 7,383,327; 7,475,282; 7,603,533; 7,636,824; 7,650,473; 7,721,138; 7,779,221; 7,831,789; 7,836,053; 7,886,120; 7,895,403; 7,934,064; 7,937,612; 7,941,510; 7,949,635; 7,953,948; 7,979,690; 8,005,797; 8,051,044; 8,069,320; 8,073,815; 8,074,035; 8,074,276; 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; 8,850,060; 8,856,927; 8,996,830; 9,213,697; 9,400,886; 9,424,678; 9,436,558; 9,471,441; 9,501,234. Zgłoszono również wnioski patentowe oczekujące na rozpatrzenie.

Wersje programu Acronis Cyber Protect 15

Program Acronis Cyber Protect 15 jest dostępny w następujących wersjach:

- Cyber Protect Essentials
- Cyber Protect Standard
- Cyber Protect Advanced
- Cyber Backup Standard
- Cyber Backup Advanced

Szczegółowe informacje na temat funkcji zawartych w poszczególnych wersjach można znaleźć w artykule Porównanie wersji programu Acronis Cyber Protect 15, w tym wdrożenia chmurowego.

Wszystkie wersje programu Acronis Cyber Protect 15 są licencjonowane według liczby chronionych obciążeń i ich typu (stacja robocza, serwer i host wirtualny). Wersje programu Cyber Protect są dostępne tylko w ramach licencji subskrypcyjnych. Wersje Cyber Backup są dostępne zarówno w ramach licencji subskrypcyjnych, jak i licencji wieczystych. Więcej informacji na temat dostępnych opcji można znaleźć w sekcji "Licencjonowanie" (s. 22).

Kluczy licencji wieczystych wersji 15 nie można używać w powiązaniu z agentami kopii zapasowych programu Acronis Cyber Backup 12.5. Agenty te jednak nadal będą działać ze swoimi starymi kluczami licencyjnymi, nawet jeśli ich serwer zarządzania zostanie zaktualizowany do wersji 15.

Licencji subskrypcyjnych oprogramowania Backup można używać w powiązaniu z agentami w wersji 12.5 nawet wtedy, gdy agenty zostaną zaktualizowane do wersji 15. Licencji subskrypcyjnych rozwiązania Cyber Protect mogą używać tylko agenty w wersji 15.

Agenty kopii zapasowych w wersji 12.5 zarejestrowane na serwerze zarządzania w wersji 15 nie mogą wykonywać operacji przetwarzania danych poza hostem, takich jak replikacja kopii zapasowych, sprawdzanie poprawności kopii zapasowych, czyszczenie lub konwersja na maszynę wirtualną.

Uwaga
Funkcje różnią się w zależności od wersji. Niektóre funkcje opisane w tej dokumentacji mogą być niedostępne w ramach używanej licencji. Szczegółowe informacje na temat funkcji zawartych w poszczególnych wersjach można znaleźć w artykule Porównanie wersji programu Acronis Cyber Protect 15, w tym wdrożenia chmurowego.

Obsługa funkcji programu Cyber Protect w poszczególnych systemach operacyjnych

Funkcje programu Cyber Protect są obsługiwane w następujących systemach operacyjnych:

- Windows: Windows 7 lub nowszy, Windows Server 2008 R2 lub nowszy.
  Zarządzanie programem antywirusowym Windows Defender jest obsługiwane w systemie Windows 8.1 lub nowszym.
- Linux: CentOS 7.x, CentOS 8.0, Virtuozzo 7.x, Acronis Cyber Infrastructure 3.x.
  Inne dystrybucje i wersje systemu Linux również mogą obsługiwać funkcje oprogramowania Cyber Protect, ale nie zostały przetestowane.
- macOS: 10.13.x lub nowszy (obsługiwana jest tylko Ochrona przed wirusami i złośliwym oprogramowaniem).

Ważne
Funkcje programu Cyber Protect są obsługiwane tylko w przypadku komputerów z zainstalowanym agentem ochrony. W przypadku maszyn wirtualnych chronionych w trybie bezagentowym, np. przez agenta dla Hyper-V, agenta dla VMware lub agenta dla Scale Computing, obsługiwane jest tylko tworzenie kopii zapasowych.

Funkcje programu Cyber Protect	Windows	Linux	macOS
Kopia zapasowa na potrzeby analizy śledczej	Tak	Nie	Nie
Ciągła ochrona danych			
Ciągła ochrona plików i folderów	Tak	Nie	Nie
Ciągła ochrona zmienianych plików przy użyciu funkcji śledzenia aplikacji	Tak	Nie	Nie
Wykrywanie automatyczne i instalacja zdalna			
Wykrywanie w sieci	Tak	Nie	Nie
Wykrywanie w domenie Active Directory	Tak	Nie	Nie
Wykrywanie w szablonach (import maszyn z pliku)	Tak	Nie	Nie
Ręczne dodawanie urządzeń	Tak	Nie	Nie
Ochrona antywirusowa firmy Acronis			
Wykrywanie oprogramowania wymuszającego okup na podstawie zachowań procesów (przy użyciu sztucznej inteligencji)	Tak	Nie	Nie
Wykrywanie procesów cryptominingu	Tak	Nie	Nie
Ochrona antywirusowa w czasie rzeczywistym	Tak	Nie	Tak
Automatycznie odzyskiwanie plików, których dotyczy problem, z lokalnej pamięci podręcznej	Tak	Nie	Nie

Ochrona własna plików kopii zapasowych Acronis	Tak	Nie	Nie
Ochrona własna oprogramowania Acronis	Tak	Nie	Nie
Statyczne analizy przenośnych plików wykonywalnych	Tak	Nie	Tak*
Ochrona dysków zewnętrznych (HDD, pamięć flash USB, karty SD)	Tak	Nie	Nie
Ochrona folderów sieciowych	Tak	Nie	Nie
Ochrona po stronie serwera	Tak	Nie	Nie
Ochrona programów Zoom, Webex, Microsoft Teams i innych narzędzi do pracy zdalnej	Tak	Nie	Nie
Skanowanie antywirusowe na żądanie	Tak	Nie	Tak
Skanuj pliki archiwum	Tak	Nie	Tak
Wykluczanie plików/folderów	Tak	Nie	Tak**
Wykluczanie procesów	Tak	Nie	Nie
Ogólnofirmowa biała lista	Tak	Nie	Tak
Wykrywanie zachowań	Tak	Nie	Nie
Kwarantanna	Tak	Nie	Tak
Filtrowanie adresów URL (http/https)	Tak	Nie	Nie
Zarządzanie programem antywirusowym Windows Defender	Tak	Nie	Nie
Zarządzanie programem Microsoft Security Essentials	Tak	Nie	Nie
Ocena luk w zabezpieczeniach			
Ocena luk w zabezpieczeniach systemu operacyjnego i jego macierzystych aplikacji	Tak	Tak***	Nie
Ocena luk w zabezpieczeniach aplikacji innych firm	Tak	Nie	Nie
Zarządzanie poprawkami			
Automatyczne zatwierdzanie poprawek	Tak	Nie	Nie
Ręczna instalacja poprawek	Tak	Nie	Nie

Planowanie automatycznych instalacji poprawek	Tak	Nie	Nie
Bezpieczne wdrażanie poprawek: utworzenie kopii zapasowej komputera przed instalacją poprawki w ramach planu ochrony	Tak	Nie	Nie
Anulowanie ponownego uruchomienia komputera podczas operacji tworzenia kopii zapasowej	Tak	Nie	Nie
Mapa ochrony danych			
Skanowanie komputerów w poszukiwaniu niechronionych plików	Tak	Nie	Nie
Przegląd niechronionych lokalizacji	Tak	Nie	Nie
Działania ochrony w ramach mapy ochrony danych	Tak	Nie	Nie
Kondycje dysków			
Kontrola kondycji dysków HDD i SSD przy użyciu sztucznej inteligencji	Tak	Nie	Nie
Inteligentne plany ochrony oparte na ostrzeżeniach z Acronis Cyber Protection Operations Center (CPOC)			
Kanał dotyczący zagrożeń	Tak	Nie	Nie
Kreator napraw	Tak	Nie	Nie
Skanowanie kopii zapasowych			
Skanowanie zaszyfrowanych kopii zapasowych	Tak	Nie	Nie
Skanowanie kopii zapasowych dysków w lokalnej pamięci masowej, udziałach sieciowych i magazynie Acronis Cloud Storage	Tak	Nie	Nie
Bezpieczne odzyskiwanie			
Skanowanie antywirusowe przy użyciu modułu firmy Acronis Ochrona przed wirusami i złośliwym oprogramowaniem podczas odzyskiwania	Tak	Nie	Nie
Pulpit zdalny			
Połączenie przez klienta opartego na HTML5	Tak	Nie	Nie
Połączenie przez macierzystego klienta RDP systemu Windows	Tak	Nie	Nie

Wymazywanie zdalne	Tak****	Nie	Nie
Cyber Protect Monitor	Tak	Nie	Tak

* W systemie macOS statyczne analizy przenośnych plików wykonywalnych są obsługiwane tylko w przypadku planowanych operacji skanowania.

** W systemie macOS wykluczenia mogą służyć tylko do wskazania plików i folderów, które nie będą skanowane w ramach ochrony w czasie rzeczywistym ani planowanych operacji skanowania.

*** Ocena luk w zabezpieczeniach zależy od dostępności oficjalnych ostrzeżeń dotyczących bezpieczeństwa dla danej dystrybucji, na przykład https://lists.centos.org/pipermail/centos-announce, https://lists.centos.org/pipermail/centos-cr-announce i innych.

**** Zdalne wymazywanie jest dostępne tylko w przypadku komputerów z systemem Windows 10 lub nowszym.

Licencjonowanie

Aby chronić obciążenie za pomocą programu Acronis Cyber Protect, trzeba mieć licencję. Do zainstalowania programu Acronis Cyber Protect nie potrzeba licencji.

Typy licencji

Program Acronis Cyber Protect jest dostępny w ramach licencji subskrypcyjnych. W okresie ich ważności, który rozpoczyna się w dniu zakupu, można bez ograniczeń korzystać z aktualizacji i bezpłatnej pomocy technicznej. Po zakończeniu okresu ważności dotychczasowe plany ochrony przestaną działać i nie będzie można tworzyć nowych planów ochrony.

Dostępne są przedłużenia dawnych licencji wieczystych. Niektóre funkcje, na przykład wdrożenia w chmurze lub tworzenie kopii zapasowych z chmury do chmury, nie są dostępne w przypadku licencji wieczystej.

Dostępna jest też licencja wersji próbnej. Zapewnia ona dostęp do wszystkich funkcji programu przez 30 dni od aktywacji.

Dodatkowe informacje na temat różnych opcji licencjonowania można znaleźć w artykule Acronis Cyber Protect 15: licensing and upgrade/downgrade FAQ (15: najczęściej zadawane pytania na temat licencjonowania oraz uaktualniania do nowszej wersji lub przechodzenia na starszą wersję) w naszej bazie wiedzy Knowledge Base. Zasady licencjonowania firmy Acronis są dostępne na stronie https://www.acronis.com/company/licensing.html.

Ważne
Wraz z rozwiązaniem Acronis Cyber Protect 15 Update 3 wprowadzono nowy model licencjonowania. Wymaga on rejestrowania licencji i aktywowania lokalnych serwerów zarządzania.

Licencjonowanie w rozwiązaniu Acronis Cyber Protect 15 Update 3 lub nowszym

W rozwiązaniu Acronis Cyber Protect 15 Update 3 lub nowszym żadnych kluczy licencyjnych nie dodaje się w konsoli lokalnej serwera zarządzania (`https://<adres IP serwera zarządzania>:<port>`).

Zamiast tego dodaje się licencje do konta w portalu Acronis Customer Portal (`https://account.acronis.com`), a następnie zarządza nimi w konsoli chmury Acronis Cyber Protect (`https://cloud.acronis.com`).

Zarządzanie licencjami serwerów zarządzania offline wymaga operacji zarówno w konsoli lokalnej, jak i w konsoli chmury.

Dodatkowe informacje o konsoli lokalnej i konsoli chmury można znaleźć w sekcji "Konto Acronis, konsola lokalna i konsola chmury" (s. 24).

Aby zacząć korzystać z serwera zarządzania z rozwiązaniem Acronis Cyber Protect 15 Update 3 lub nowszym

1. Dodaj co najmniej jedną licencję do konta w portalu Acronis Customer Portal (https://account.acronis.com).
   Licencje kupione online są automatycznie dodawane do tego konta.
2. [W przypadku trybu wdrożenia lokalnego] Aktywuj serwer zarządzania.
3. Przydziel licencję do serwera zarządzania.

Typy serwerów zarządzania

W zależności od trybu wdrożenia można używać następujących typów serwerów zarządzania:

- Chmurowy serwer zarządzania
- Lokalny serwer zarządzania
  - Serwer zarządzania online
  - Serwer zarządzania offline

Na koncie Acronis można mieć więcej niż jeden serwer zarządzania. Można też zastosować mieszany tryb wdrożenia: z chmurowym i lokalnym serwerem zarządzania.

Jeśli używasz wielu serwerów zarządzania, możesz podzielić limit licencji między nie. Dodatkowe informacje na ten temat można znaleźć w sekcji "Przenoszenie limitu licencji na inny serwer zarządzania" (s. 34).

Chmurowy serwer zarządzania

W przypadku wdrożenia chmurowego nie trzeba instalować ani utrzymywać serwera zarządzania w swojej sieci. Korzysta się z serwera zarządzania wdrożonego już w centrum danych firmy Acronis i trzeba tylko zainstalować agenty ochrony na potrzeby swoich obciążeń.

Chmurowy serwer zarządzania nie wymaga aktywacji. Jest zawsze online, a informacje o licencjonowaniu są automatycznie synchronizowane między serwerem a kontem Acronis.

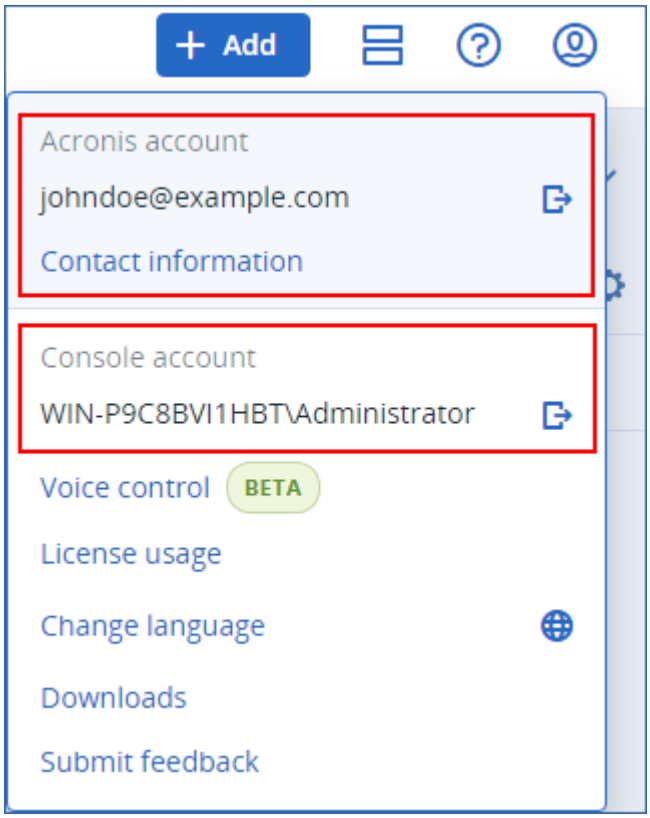
Lokalny serwer zarządzania

W przypadku wdrożenia lokalnego instaluje się w swojej sieci zarówno serwer zarządzania, jak i agenty ochrony. Można mieć serwer zarządzania offline, który nie ma połączenia z Internetem, lub serwer zarządzania online, który ma połączenie z Internetem.

Lokalne serwery zarządzania wymagają aktywacji. Dodatkowe informacje o aktywacji można znaleźć w sekcji "Aktywowanie serwera zarządzania" (s. 28).

Uwaga

W konsoli lokalnej aktywowanego lokalnego serwera zarządzania są widoczne dwa konta: konto Acronis, używane do synchronizacji informacji o licencjonowaniu, oraz konto konsoli, używane w celu uzyskiwania dostępu właśnie do konsoli lokalnej.



Lokalny serwer zarządzania online

Aktywacja serwera zarządzania online odbywa się przez Internet: przez zalogowanie się na koncie Acronis po uzyskaniu dostępu do konsoli lokalnej po raz pierwszy.

Lokalny serwer zarządzania offline

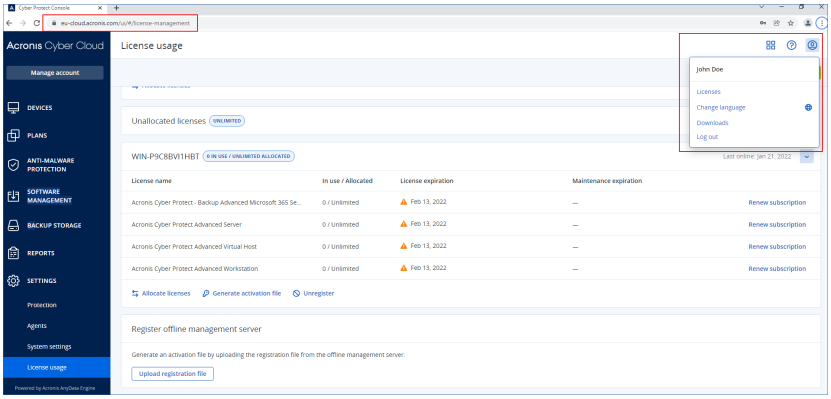
Aktywacja serwera zarządzania offline i synchronizacja jego informacji o licencjonowaniu z kontem Acronis jest wykonywana ręcznie, przy użyciu pliku.

Konto Acronis, konsola lokalna i konsola chmury

Aby korzystać z programu Acronis Cyber Protect i zarządzać licencjami oraz ich wykorzystaniem, trzeba mieć konto Acronis. Na tym koncie są zarejestrowane wszystkie Twoje licencje i serwery zarządzania.

Za pomocą tego konta można uzyskać dostęp do następujących konsol:

- Konsola chmury (`https://cloud.acronis.com`)

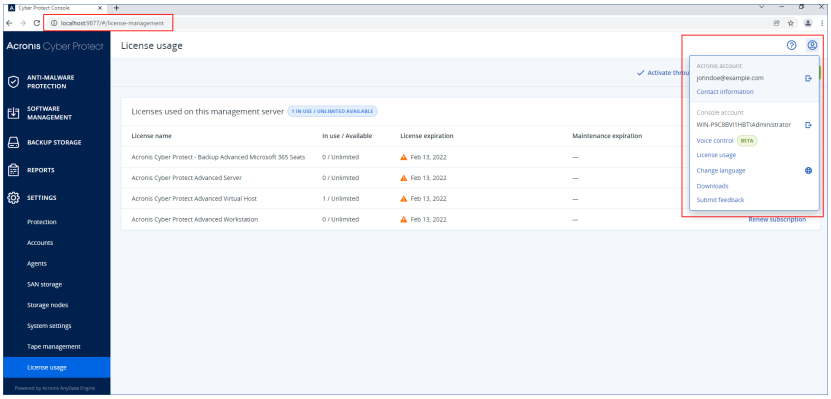


Uwaga

Gdy zalogujesz się do konsoli chmury, jej adres URL ulegnie zmianie i zostanie wyświetlone centrum danych, do którego należy Twoje konto. Na przykład `https://eu-cloud.acronis.com` lub `https://jp-cloud.acronis.com`.

Konsola chmury jest głównym miejscem, w którym możesz zarządzać swoimi licencjami. Na karcie **Ustawienia** > **Wykorzystanie licencji** można przydzielić dostępne licencje i limit licencji do określonego serwera zarządzania, przenieść przydział licencji lub limitów licencji na inny serwer zarządzania bądź sfinalizować rejestrację serwerów zarządzania offline.

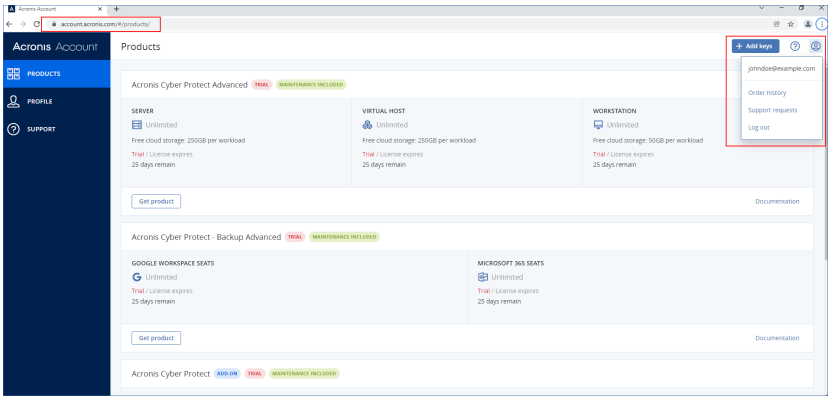
- Konsola lokalna lokalnego serwera zarządzania (`https://<adres IP serwera zarządzania>:<port>`)



W tym miejscu można sprawdzać przydzielone licencje, ich limit i wykorzystanie oraz datę wygaśnięcia.

Konsola lokalna oraz konsola chmury są używane podczas aktywacji serwera zarządzania offline lub przydzielania do niego licencji.

- Acronis Customer Portal (`https://account.acronis.com`)



W portalu Acronis Customer Portal można zarządzać kupionymi produktami, na przykład sprawdzić datę wygaśnięcia subskrypcji, dodać nowe klucze licencyjne, zarejestrować przedłużenie licencji lub zamówić uaktualnienie do nowszej wersji. Można też skontaktować się z zespołem pomocy technicznej, pobrać pliki instalacyjne produktu oraz uzyskać dostęp do dokumentacji produktu.

Zarządzanie licencjami

Poniższa tabela zawiera zestawienie dostępnych operacji i miejsc ich wykonywania.

Operacja	Lokalizacja
Dodawanie licencji do konta	Licencje dodaje się w portalu Acronis Customer Portal (`https://account.acronis.com`). Licencje kupione online są tam dodawane automatycznie.
Aktywowanie serwera zarządzania	Serwer zarządzania aktywuje się przez zarejestrowanie go na koncie. Serwer zarządzania online aktywuje się w jego konsoli lokalnej (`https://<adres IP serwera zarządzania>:<port>`) przez zalogowanie się do konta Acronis. Aktywacja serwera zarządzania offline wymaga wykonania operacji zarówno w konsoli lokalnej, jak i w konsoli chmury.
Przydzielanie licencji do serwera zarządzania Modyfikowanie obecnego przydziału licencji	Na serwerach zarządzania online licencje przydziela się za pomocą konsoli chmury (`https://cloud.acronis.com`). Przydzielone licencje są automatycznie synchronizowane z serwerem zarządzania. Na serwerze zarządzania offline licencje przydziela się za pomocą pliku aktywacyjnego. Procedura wymaga użycia zarówno konsoli lokalnej serwera zarządzania (`https://<adres IP serwera zarządzania>:<port>`), jak i konsoli chmury (`https://cloud.acronis.com`).
Przypisywanie licencji do obciążeń	Ta operacja jest wykonywana automatycznie.
Wyrejestrowywanie serwera zarządzania z konta	Serwery zarządzania online można wyrejestrować za pomocą konsoli chmury (`https://cloud.acronis.com`). Wyrejestrowanie serwera zarządzania offline odbywa się za pomocą pliku

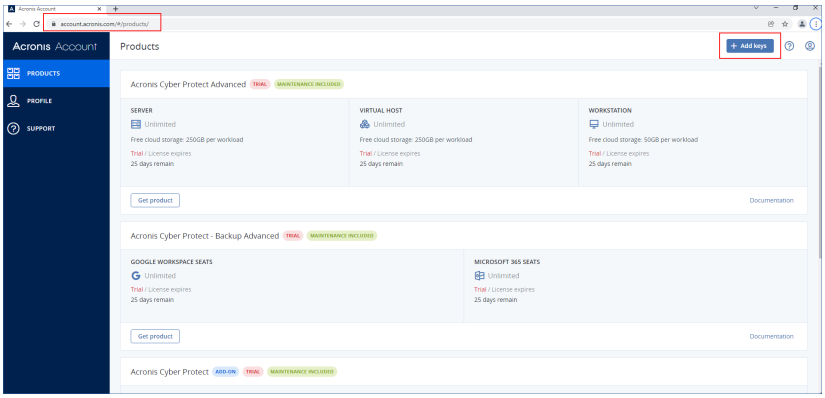
Operacja	Lokalizacja
	dezaktywacyjnego. Procedura wymaga użycia zarówno konsoli lokalnej serwera zarządzania offline (`https://<adres IP serwera zarządzania>:<port>`), jak i konsoli chmury (`https://cloud.acronis.com`). Aby wyrejestrować serwer zarządzania offline, do którego nie masz dostępu, należy użyć tylko konsoli chmury.

Dodawanie licencji do konta Acronis

Aby korzystać z licencji, trzeba ją dodać do konta Acronis. Licencje kupione online są automatycznie dodawane do konta. Licencje kupione offline trzeba dodać ręcznie.

Aby dodać licencję na koncie Acronis

1. Zaloguj się do portalu Acronis Customer Portal (`https://account.acronis.com`) przy użyciu swoich poświadczeń użytkownika konta Acronis.
2. W menu nawigacyjnym kliknij **Produkty**.
3. Kliknij **Dodaj klucze**.



4. Wprowadź klucze licencyjne — każdy w osobnym wierszu — i kliknij **Dodaj**.

> **Uwaga**
> Można wprowadzić maksymalnie 100 kluczy licencyjnych naraz.

Licencje zostaną dodane do konta i można zarządzać ich wykorzystaniem w konsoli chmury (`https://cloud.acronis.com`).

Ważne
Zanim zaktualizujesz rozwiązanie do wersji Acronis Cyber Protect 15 Update 3, wyeksportuj lokalnie przechowywane licencje wieczyste do pliku, a następnie dodaj je do konta Acronis.

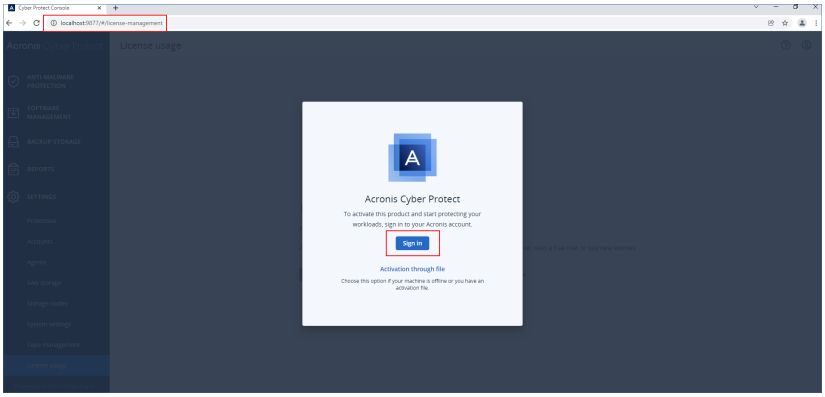
Aby sprawdzić klucze licencyjne wprowadzone lokalnie na serwerze zarządzania, przejdź do sekcji `https://<adres IP serwera zarządzania>:<port>/api/account_server/v2/licensing/legacy/license_keys`.

Aktywowanie serwera zarządzania

Serwer zarządzania aktywuje się przez zarejestrowanie go na swoim koncie Acronis.

Aby aktywować serwer zarządzania online

1. Po zainstalowaniu serwera zarządzania Acronis Cyber Protect otwórz jego konsolę lokalną (`https://<adres IP serwera zarządzania>:<port>`).
2. W nowo otwartym oknie dialogowym kliknij **Zaloguj się**.



3. Zaloguj się na koncie Acronis.

W wyniku tych działań serwer zarządzania zostanie automatycznie zarejestrowany i aktywowany.

Aby rozpocząć ochronę obciążeń, przydziel do tego serwera co najmniej jedną licencję. Dodatkowe informacje na temat przydzielania licencji można znaleźć w sekcji "Przydzielanie licencji do serwera zarządzania" (s. 31).

Uwaga
Serwery zarządzania online wymagają dostępu do Internetu, aby synchronizować informacje o licencjonowaniu z kontem Acronis. Jeśli taki serwer pozostanie w trybie offline przez ponad 30 dni, jego plany ochrony przestaną działać i obciążenia przestaną być chronione.

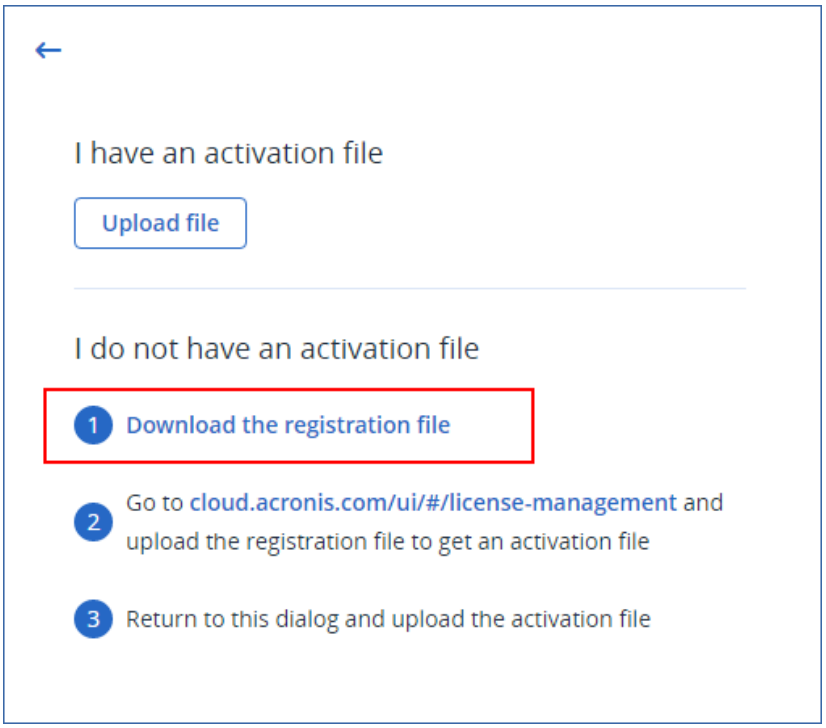
Jeśli wylogujesz się z konta Acronis w konsoli lokalnej, informacje o licencjonowaniu nie będą mogły zostać zsynchronizowane. Jeśli nie zalogujesz się ponownie w ciągu 30 dni, plany ochrony przestaną działać i obciążenia przestaną być chronione.

Aby aktywować serwer zarządzania offline

Aktywacja serwera zarządzania offline wymaga wykonania operacji zarówno w konsoli lokalnej, jak i w konsoli chmury.

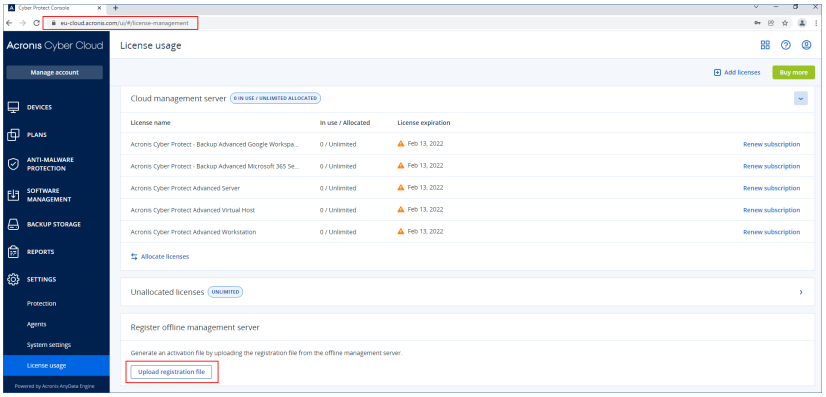
Aby uzyskać dostęp do konsoli chmury, potrzebny jest drugi komputer podłączony do Internetu.

1. Po zainstalowaniu serwera zarządzania Acronis Cyber Protect otwórz jego konsolę lokalną (`https://<adres IP serwera zarządzania>:<port>`).
2. W nowo otwartym oknie dialogowym kliknij **Aktywacja przy użyciu pliku**.
3. W obszarze **Nie mam pliku aktywacyjnego** kliknij **Pobierz plik rejestracji**.



Plik rejestracji zostanie pobrany na komputer.

4. Na komputerze z dostępem do Internetu zaloguj się do konsoli chmury (`https://cloud.acronis.com`) i przejdź do sekcji **Ustawienia** > **Wykorzystanie licencji**.
5. W sekcji **Zarejestruj serwer zarządzania offline** kliknij **Prześlij plik rejestracji**.



6. W nowo otwartym oknie dialogowym kliknij **Przeglądaj**, a następnie wybierz plik rejestracji pobrany z serwera zarządzania offline.
7. W nowo otwartym oknie dialogowym kliknij **Pobierz plik**.

   Plik aktywacyjny zostanie pobrany na komputer.

Ważne

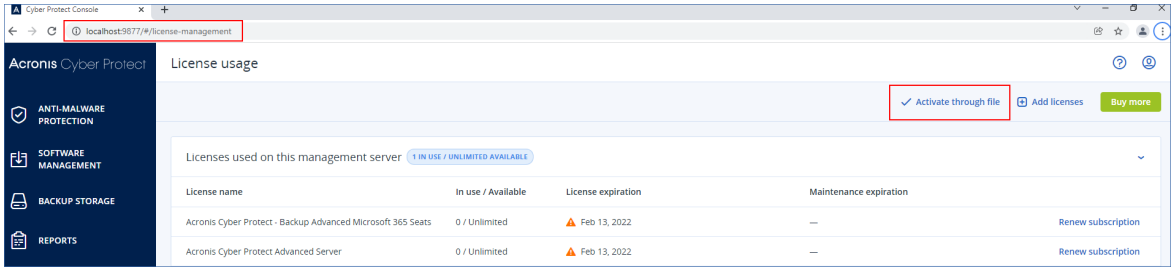
Jeśli dany serwer zarządzania offline jest jedynym serwerem zarządzania w środowisku, licencje znajdujące się na koncie Acronis zostaną automatycznie do niego przydzielone. Plik aktywacyjny będzie zawierać te informacje, więc dodatkowe przydzielanie nie jest konieczne.

Jeśli nie jest to jedyny serwer zarządzania w środowisku, po aktywacji trzeba będzie przydzielić licencje zgodnie z instrukcją podaną w sekcji "Przydzielanie licencji do serwera zarządzania" (s. 31).

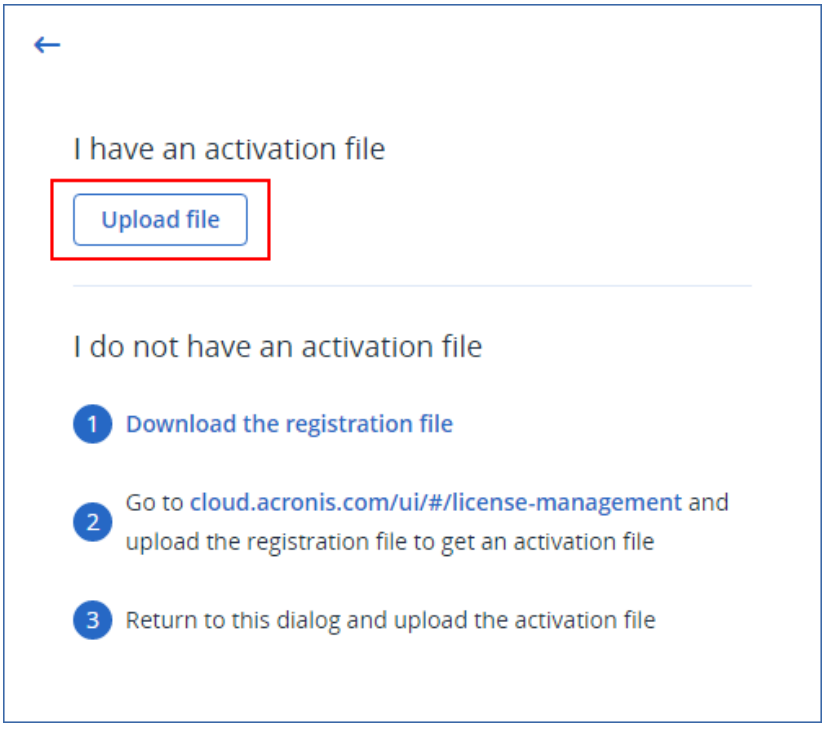
8. W konsoli lokalnej serwera zarządzania offline (`https://<adres IP serwera zarządzania>:<port>`) przejdź do okna dialogowego **Aktywacja przy użyciu pliku**.

Uwaga

Jeśli okno dialogowe **Aktywacja przy użyciu pliku** nie jest otwarte, wybierz **Ustawienia** > **Wykorzystanie licencji**, a następnie kliknij **Aktywuj przy użyciu pliku**.



9. W obszarze **Mam plik aktywacyjny** kliknij **Prześlij plik** i wybierz plik aktywacyjny pobrany z konsoli chmury.



W wyniku tych działań serwer zarządzania offline zostanie zarejestrowany na koncie Acronis i aktywowany.

Uwaga
W przypadku serwera zarządzania działającego na maszynie wirtualnej, której identyfikator UUID nie jest unikatowy, aktywacja może być niemożliwa. Identyfikator UUID maszyny wirtualnej mógł na przykład zostać zduplikowany podczas jej klonowania lub konwersji za pomocą narzędzia VMware vCenter Converter. W razie napotkania tego typu problemu skontaktuj się z naszym zespołem pomocy technicznej.

Dodatkowe informacje na temat zapobiegania duplikowaniu identyfikatora UUID na maszynach wirtualnych VMware można znaleźć w artykule Editing a virtual machine with a duplicate UUID.bios (1002403) (Edytowanie maszyny wirtualnej ze zduplikowanym UUID.bios (1002403)).

Przydzielanie licencji do serwera zarządzania

Aby skorzystać z licencji, należy przydzielić jej limit lub część jej limitu do serwera zarządzania. Do serwera zarządzania można przydzielić więcej niż jedną licencję. Można też podzielić limit licencji i przydzielić jego części różnym serwerom zarządzania.

Uwaga
Jeśli na koncie Acronis jest tylko jeden serwer zarządzania, wszystkie licencje zostaną automatycznie przydzielone do tego serwera. Informacje na temat przenoszenia przydziału licencji na inny serwer zarządzania można znaleźć w sekcji "Przenoszenie limitu licencji na inny serwer zarządzania" (s. 34).

Jeśli na koncie Acronis jest więcej niż jeden serwer zarządzania, nowe licencje będą widoczne w sekcji **Nieprzydzielone licencje** w konsoli chmury (`https://cloud.acronis.com`). Licencje te należy przydzielić ręcznie.

Wszystkie operacje dotyczące licencji są automatycznie synchronizowane z serwerami zarządzania online. Aby zsynchronizować zmianę przydziału z serwerem zarządzania offline, należy utworzyć nowy plik aktywacyjny, a następnie powtórzyć procedurę przydzielania. Dodatkowe informacje o różnych serwerach zarządzania można znaleźć w sekcji "Typy serwerów zarządzania" (s. 23).

Aby przydzielić licencje do serwera zarządzania online

1. W konsoli chmury (`https://cloud.acronis.com`) kliknij **Ustawienia** > **Wykorzystanie licencji**.
2. Przejdź do serwera zarządzania, do którego chcesz przydzielić licencję.
3. Kliknij **Przydziel licencje**.
4. W nowo otwartym oknie dialogowym wskaż licencję i limit licencji, które chcesz przydzielić do serwera.
5. Kliknij **Zapisz**.

W wyniku tych działań informacje o licencjonowaniu zostaną automatycznie zsynchronizowane z serwerem zarządzania i będzie można używać przydzielonej licencji do ochrony obciążeń.

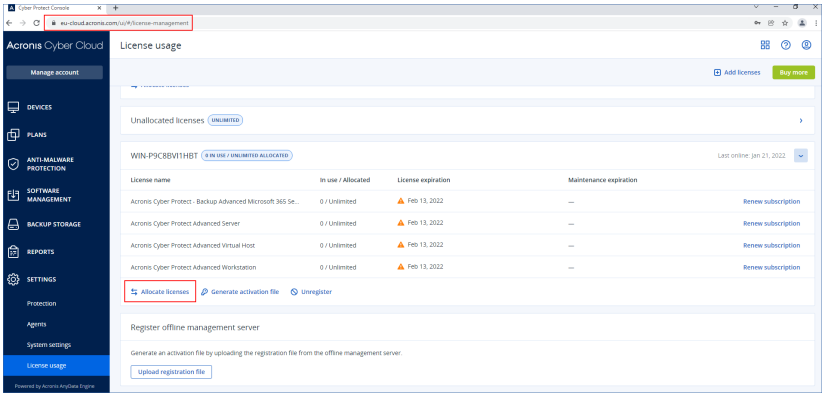
Aby zmodyfikować przydział, ponownie wykonaj powyższą procedurę.

Ważne
Jeśli zmodyfikowany limit licencji jest mniejszy niż liczba agentów ochrony, najmniej ładowane agenty przestaną działać. Są one wybierane automatycznie. Jeśli to nie odpowiada Twoim potrzebom, ręcznie zmień przypisania dostępnych licencji.

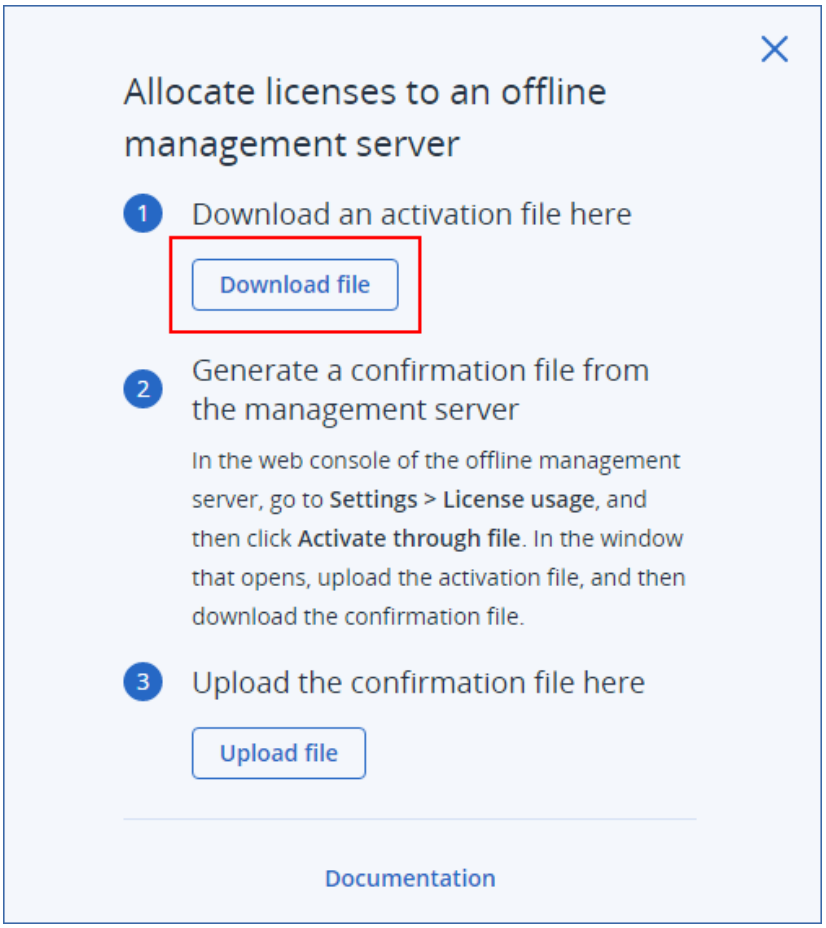
Aby przydzielić licencje do serwera zarządzania offline

Aby przydzielić licencje do serwera zarządzania offline, trzeba użyć zarówno konsoli chmury, jak i konsoli lokalnej. Aby uzyskać dostęp do konsoli chmury, potrzebny jest drugi komputer podłączony do Internetu.

1. Na komputerze z dostępem do Internetu zaloguj się do konsoli chmury (`https://cloud.acronis.com`) i kliknij **Ustawienia** > **Wykorzystanie licencji**.
2. Przejdź do serwera zarządzania, do którego chcesz przydzielić licencję.
3. Kliknij **Przydziel licencje**.

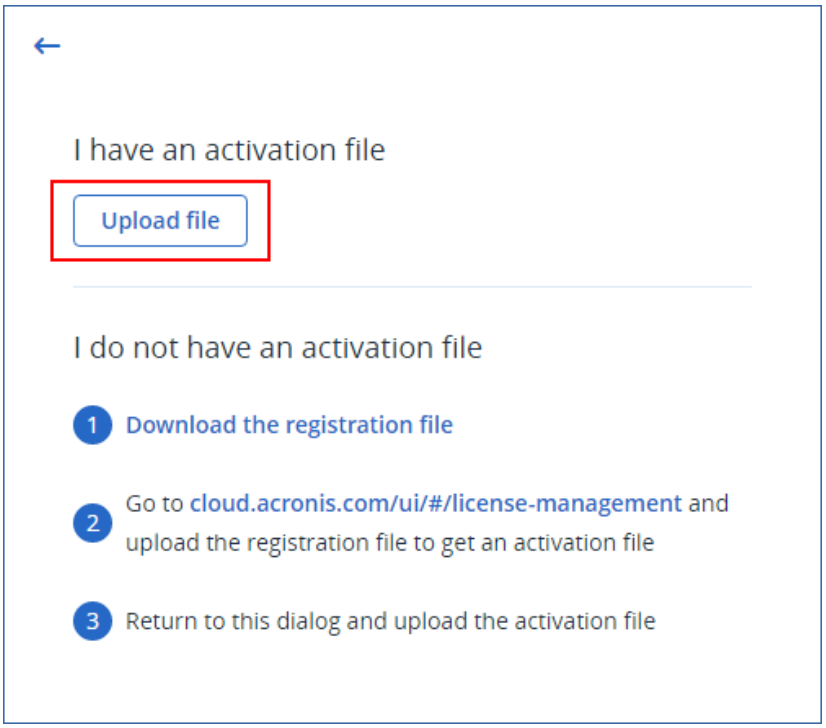


4. W nowo otwartym oknie dialogowym wskaż licencję i limit licencji, które chcesz przydzielić do serwera.
5. Kliknij **Zapisz**.
6. W oknie dialogowym **Przydziel licencje do serwera zarządzania offline** kliknij **Pobierz plik**.



Plik aktywacyjny zostanie pobrany na komputer.

7. W konsoli lokalnej serwera zarządzania offline (`https://<adres IP serwera zarządzania>:<port>`) przejdź do sekcji **Ustawienia** > **Wykorzystanie licencji**, a następnie kliknij **Aktywuj przy użyciu pliku**.
8. W nowo otwartym oknie dialogowym w obszarze **Mam plik aktywacyjny** kliknij **Prześlij plik** i wybierz plik aktywacyjny pobrany z konsoli chmury.



W wyniku tych działań informacje o licencjonowaniu zostaną zsynchronizowane między kontem Acronis a serwerem zarządzania offline.

Aby zwiększyć przydzielony limit licencji, ponownie wykonaj powyższą procedurę.

Aby zmniejszyć przydzielony limit licencji, zapoznaj się z sekcją "Zmniejszanie limitu licencji przydzielonych do serwera zarządzania offline" (s. 35).

Przenoszenie limitu licencji na inny serwer zarządzania

Limit licencji można przenieść z jednego serwera zarządzania na drugi. Opcja ta może się przydać w sytuacji, gdy licencje przydzielone do serwera zarządzania nie są wykorzystywane przez żadne obciążenie lub gdy potrzeba więcej licencji w przypadku innego serwera zarządzania.

Uwaga
Jeśli na koncie Acronis jest tylko jeden serwer zarządzania, wszystkie licencje zostaną automatycznie przydzielone do tego serwera.

Jeśli na koncie Acronis jest więcej niż jeden serwer zarządzania, nowe licencje będą widoczne w sekcji **Nieprzydzielone licencje** w konsoli chmury (`https://cloud.acronis.com`). Licencje te należy przydzielić ręcznie.

Aby przenieść limit licencji na inny serwer zarządzania

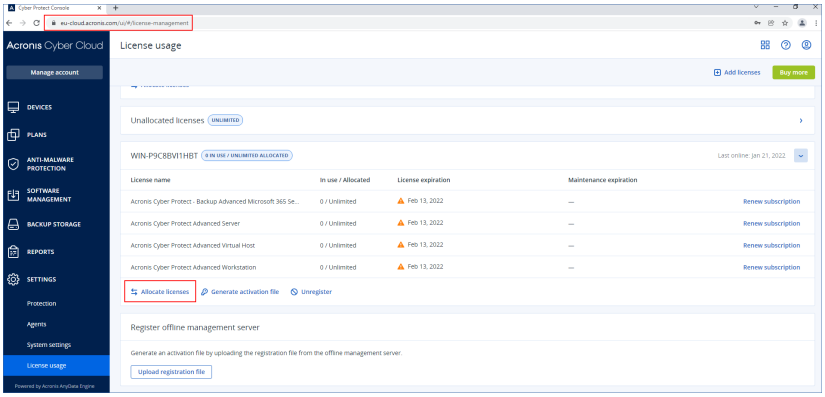
1. Zmniejsz limit licencji przydzielony do pierwotnego serwera zarządzania, postępując zgodnie z instrukcją opisaną w sekcji "Przydzielanie licencji do serwera zarządzania" (s. 31).
   Zwolnione limity licencji będą widoczne w sekcji **Nieprzydzielone licencje** w konsoli chmury.

2. Przydziel limit licencji do drugiego serwera zarządzania, postępując zgodnie z instrukcją opisaną w sekcji "Przydzielanie licencji do serwera zarządzania" (s. 31).

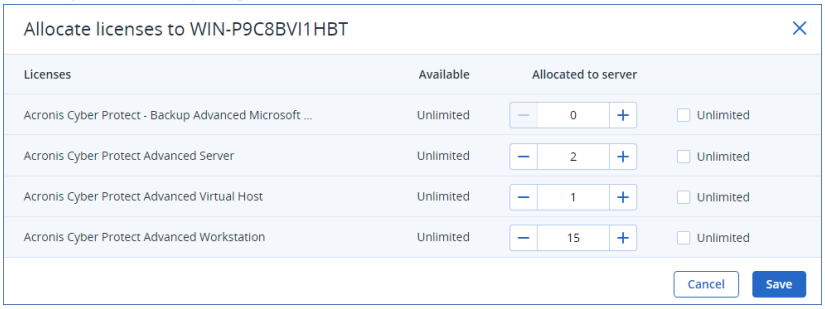
Zmniejszanie limitu licencji przydzielonych do serwera zarządzania offline

Aby zmniejszyć limit licencji przydzielony do serwera zarządzania offline, trzeba użyć zarówno konsoli chmury, jak i konsoli lokalnej. Aby uzyskać dostęp do konsoli chmury, potrzebny jest drugi komputer podłączony do Internetu.

1. Na komputerze z dostępem do Internetu zaloguj się do konsoli chmury (`https://cloud.acronis.com`) i kliknij **Ustawienia** > **Wykorzystanie licencji**.
2. Przejdź do serwera zarządzania, do którego chcesz przydzielić licencję, a następnie kliknij **Przydziel licencje**.

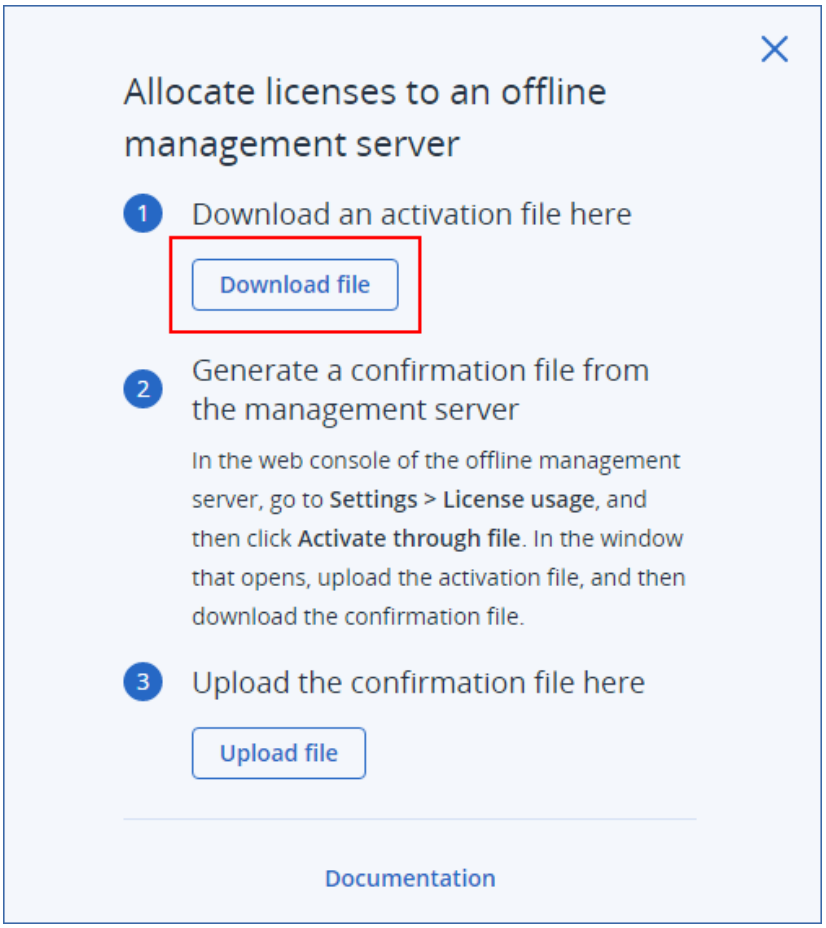


3. W nowo otwartym oknie dialogowym zmień licencje i limity licencji przydzielone do serwera, a następnie kliknij **Zapisz**.



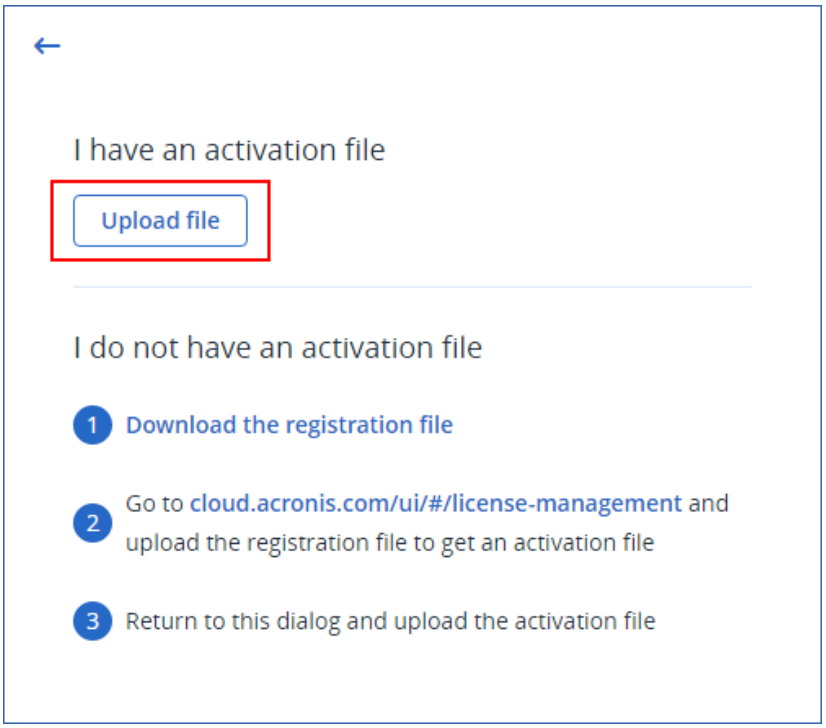
Nowy przydział rozpocznie oczekiwanie na realizację. Aby go anulować, kliknij **Usuń ten przydział**.

4. W oknie dialogowym **Przydziel licencje do serwera zarządzania offline** kliknij **Pobierz plik**.

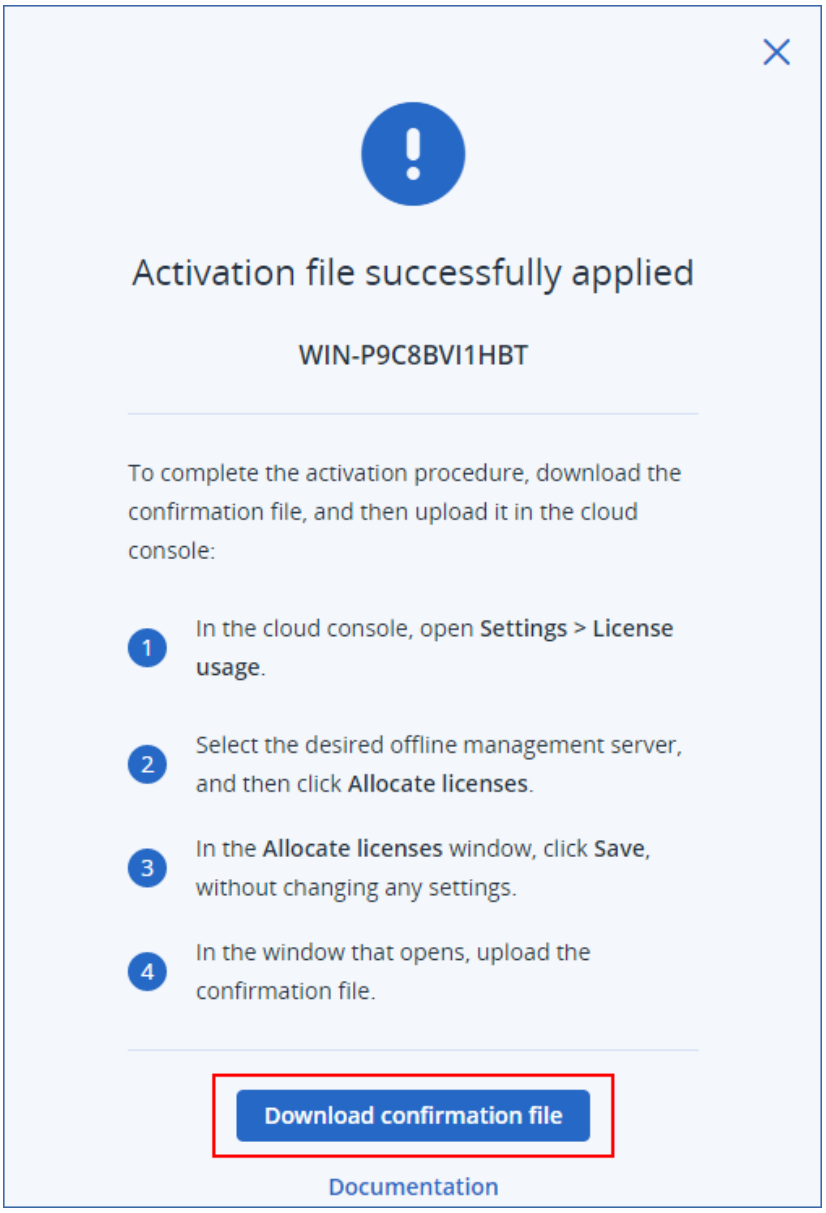


Plik aktywacyjny zostanie pobrany na komputer.

5. W konsoli lokalnej serwera zarządzania offline (`https://<adres IP serwera zarządzania>:<port>`) przejdź do sekcji **Ustawienia** > **Wykorzystanie licencji**, a następnie kliknij **Aktywuj przy użyciu pliku**.
6. W nowo otwartym oknie dialogowym w obszarze **Mam plik aktywacyjny** kliknij **Prześlij plik** i wybierz plik aktywacyjny pobrany z konsoli chmury.

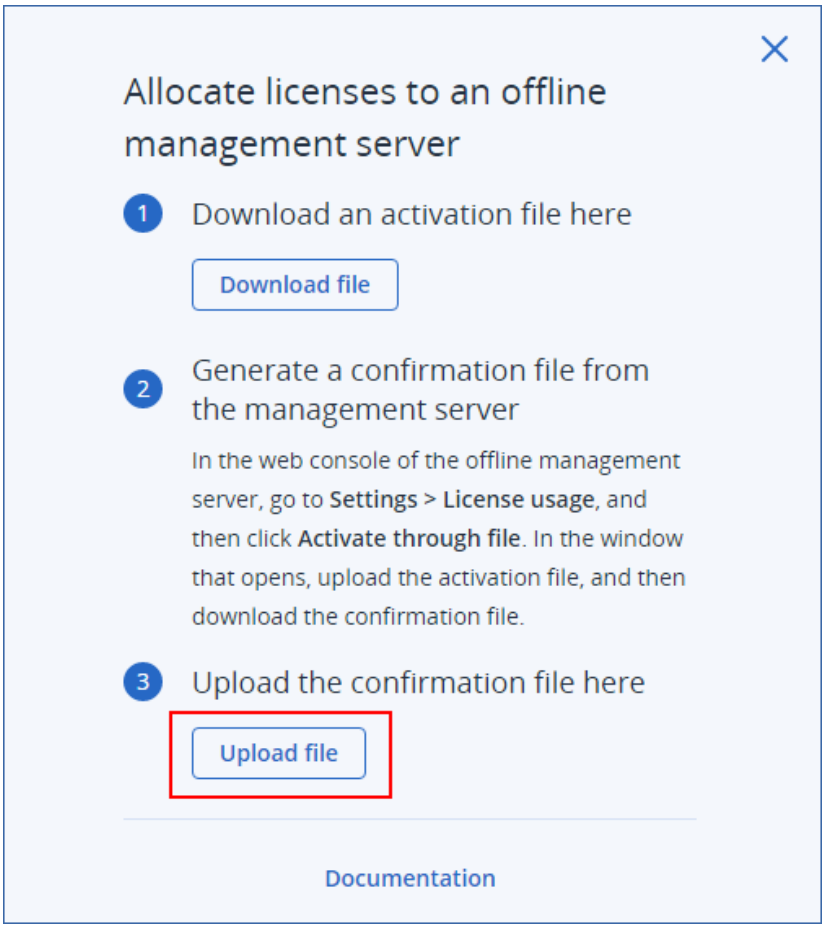


7. W nowo otwartym oknie dialogowym kliknij **Pobierz plik potwierdzenia**.



Plik potwierdzenia zostanie pobrany na komputer.

8. W konsoli chmury (`https://cloud.acronis.com`) kliknij **Ustawienia** > **Wykorzystanie licencji**.
9. Przejdź do serwera zarządzania, do którego chcesz przydzielić licencję, a następnie kliknij **Przydziel licencje**.
10. W nowo otwartym oknie dialogowym kliknij **Zapisz** bez zmieniania jakichkolwiek ustawień.
11. W oknie dialogowym **Przydziel licencje do serwera zarządzania offline** kliknij **Prześlij plik**, a następnie wybierz plik potwierdzenia pobrany z serwera zarządzania offline.



W wyniku tych działań informacje o licencjonowaniu zostaną zsynchronizowane między kontem Acronis a serwerem zarządzania offline.

Ważne
Jeśli zmodyfikowany limit licencji jest mniejszy niż liczba agentów ochrony, najmniej ładowane agenty przestaną działać. Są one wybierane automatycznie. Jeśli to nie odpowiada Twoim potrzebom, ręcznie zmień przypisania dostępnych licencji.

Przypisywanie licencji do obciążeń

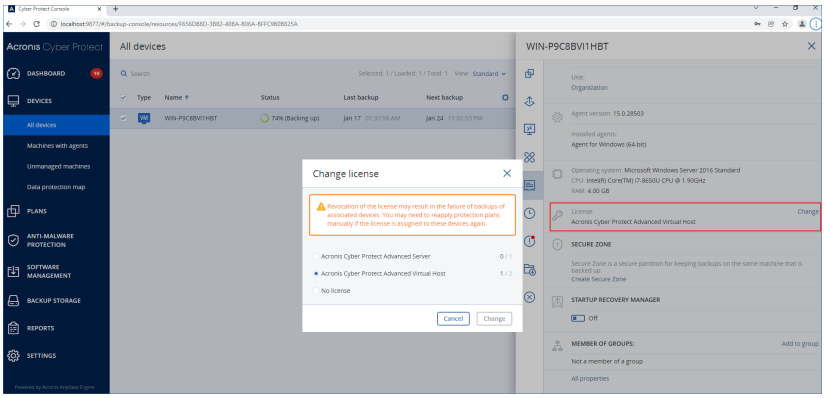
Serwer zarządzania rozdziela przydzielone licencje między zarejestrowane na nim obciążenia.

Serwer zarządzania przypisuje licencję do obciążenia przy pierwszym zastosowaniu planu ochrony do tego obciążenia. Jeśli do serwera zarządzania przydzielono więcej niż jedną licencję, przypisuje on obciążeniu najbardziej odpowiednią licencję na podstawie typu obciążenia, systemu operacyjnego i wymaganego poziomu ochrony.

Aby sprawdzić przypisaną licencję, w konsoli internetowej serwera zarządzania wybierz odpowiednie obciążenie i kliknij **Szczegóły**.

Aby ręcznie zmienić przypisanie licencji do obciążenia

1. W konsoli internetowej serwera zarządzania kliknij **Urządzenia**, a następnie wybierz odpowiednie obciążenie.
2. Kliknij opcję **Szczegóły**.
3. [W przypadku lokalnych serwerów zarządzania] Przejdź do sekcji **Licencja** i kliknij **Zmień**.
4. [W przypadku serwerów zarządzania w chmurze] Przejdź do sekcji **Limit usług** i kliknij **Zmień**.
5. Wybierz odpowiednią licencję (limit usług) i kliknij **Zmień**.



Ograniczenia

W przypadku serwerów zarządzania offline bieżące wykorzystanie limitu licencji jest widoczne tylko w konsoli lokalnej. Serwery zarządzania offline nie synchronizują tych danych z kontem Acronis i nie są one dostępne w konsoli chmury.

Znane problemy

W konsoli chmury wykorzystanie lub przypisanie licencji **Host wirtualny** może być niepoprawnie wyświetlane. Dodatkowe informacje można znaleźć w tym artykule bazy wiedzy Knowledge Base.

Wyrejestrowywanie serwera zarządzania

Aby wyrejestrować serwer zarządzania online

1. W konsoli chmury (`https://cloud.acronis.com`) kliknij **Ustawienia** > **Wykorzystanie licencji**.
2. Przejdź do odpowiedniego serwera zarządzania i kliknij **Wyrejestruj**.
3. Zostanie wyświetlone okno **Wyrejestruj serwer zarządzania**.
4. Wprowadź adres e-mail powiązany z kontem, aby potwierdzić wyrejestrowanie.
5. Kliknij **Wyrejestrowanie**.

W wyniku tych działań wszystkie licencje, które zostały przydzielone do wyrejestrowanego serwera, zostaną zwolnione i będzie można je przydzielić do innego serwera zarządzania dostępnego na koncie. W konsoli lokalnej wyrejestrowanego serwera zarządzania licencje zostaną wyzerowane.

Aby wyrejestrować serwer zarządzania offline

Istnieją dwa punkty wejścia umożliwiające wyrejestrowanie serwera zarządzania w trybie offline:

Konsola lokalna:

1. W konsoli lokalnej kliknij **Wyrejestruj** w wierszu konta. Zostanie wyświetlone okno **Wyrejestruj serwer zarządzania**.
2. W polu **Nazwa logowania** wpisz adres e-mail powiązany z lokalnym administratorem.
3. Kliknij **Wyrejestruj**.
4. Zostanie wyświetlony wyskakujący ekran **Pomyślnie wyrejestrowano**.
5. Kliknij **Pobierz plik wyrejestrowania**.
6. W konsoli chmury kliknij **Wyrejestruj**. Zostanie wyświetlone okno **Wyrejestruj serwer zarządzania**.
7. Kliknij **Wyrejestruj serwer zarządzania offline**. Zostanie wyświetlone okno **Wyrejestruj serwer zarządzania offline**.
8. Kliknij **Przeglądaj**, a następnie wybierz plik wyrejestrowania pobrany z konsoli lokalnej.
9. Kliknij **Wyrejestruj**.

Konsola chmury:

1. Na komputerze z dostępem do Internetu zaloguj się do konsoli chmury (`https://cloud.acronis.com`) i kliknij **Ustawienia** > **Wykorzystanie licencji**.
2. Przejdź do odpowiedniego serwera zarządzania i kliknij **Wyrejestruj**. Zostanie wyświetlone okno **Wyrejestruj serwer zarządzania**.
3. Kliknij **Wyrejestruj serwer zarządzania offline**. Zostanie wyświetlone okno **Wyrejestruj serwer zarządzania offline**.
4. W konsoli lokalnej serwera zarządzania, który chcesz wyrejestrować (`https://<adres IP serwera zarządzania>:<port>`), przejdź do sekcji **Ustawienia** > **Wykorzystanie licencji**, a następnie kliknij **Wyrejestruj**. Plik wyrejestrowania zostanie pobrany na komputer.
5. W konsoli chmury wróć do okna **Wyrejestruj serwer zarządzania offline**.
6. Kliknij **Przeglądaj**, a następnie wybierz plik wyrejestrowania pobrany z konsoli lokalnej.
7. Kliknij **Wyrejestruj**.
8. Jeśli nie masz już dostępu do komputera, na którym jest zainstalowany serwer zarządzania, możesz też kliknąć **Nie mam dostępu do komputera z serwerem zarządzania**.

   Ostrzeżenie!
   Komputer ten zostanie na stałe zablokowany i usunięty z Twojego konta. Nie będzie już można zarejestrować na nim serwera zarządzania.

W wyniku tych działań wszystkie licencje, które zostały przydzielone do wyrejestrowanego serwera, zostaną zwolnione i będzie można je przydzielić do innego serwera zarządzania dostępnego na koncie. W konsoli lokalnej wyrejestrowanego serwera zarządzania licencje zostaną wyzerowane.

Licencjonowanie w rozwiązaniu Acronis Cyber Protect 15 Update 2 lub starszym

Aby korzystać z rozwiązania Acronis Cyber Protect w wersji 15 Update 2 lub starszej, trzeba dodać do serwera zarządzania co najmniej jeden klucz licencyjny. Licencja jest automatycznie przypisywana do komputera po zastosowaniu planu ochrony.

Licencje można również przypisywać i odwoływać ręcznie. Ręczne operacje na licencjach są dostępne tylko w przypadku administratorów organizacji. Dodatkowe informacje o administratorach można znaleźć w sekcji "Jednostki i konta administracyjne" (s. 666).

Dodawanie kluczy licencyjnych do serwera zarządzania

W rozwiązaniu Acronis Cyber Protect 15 Update 2 lub starszym dodaje się klucze licencyjne do serwera zarządzania.

Aby dodać klucze licencyjne do serwera zarządzania

1. W konsoli internetowej Cyber Protect przejdź do sekcji **Ustawienia** > **Licencje**.
2. Kliknij **Dodaj klucze**.
3. Wprowadź klucze licencyjne — każdy w osobnym wierszu.
4. Kliknij **Dodaj**.
5. [W przypadku dodawania kluczy licencji subskrypcyjnych] Aby aktywować licencję subskrypcyjną, zaloguj się na koncie Acronis.
   a. W formularzu logowania wprowadź poświadczenia, których używasz w portalu Acronis Customer Portal (`https://account.acronis.com`), a następnie kliknij **Zaloguj się**.
   b. Potwierdź konto i kliknij **Synchronizacja**.
   c. Po zakończeniu operacji kliknij **Gotowe**.
6. W panelu **Dodaj klucze licencyjne** kliknij **Gotowe**.

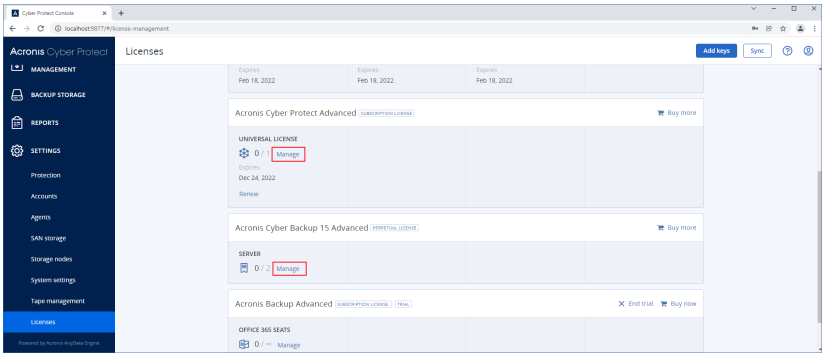
Uwaga
Klucze licencji subskrypcyjnych zarejestrowane na koncie Acronis można zaimportować automatycznie, zamiast ponownie dodawać do serwera zarządzania. Aby zaimportować klucze licencyjne, w panelu **Dodaj klucze licencyjne** kliknij **Synchronizuj z kontem Acronis**, a następnie zaloguj się na koncie Acronis.

Zarządzanie licencjami subskrypcyjnymi

Przed przypisaniem licencji do obciążenia trzeba dodać klucz licencyjny do serwera zarządzania. Dodatkowe informacje na ten temat można znaleźć w sekcji "Dodawanie kluczy licencyjnych do serwera zarządzania" (s. 42).

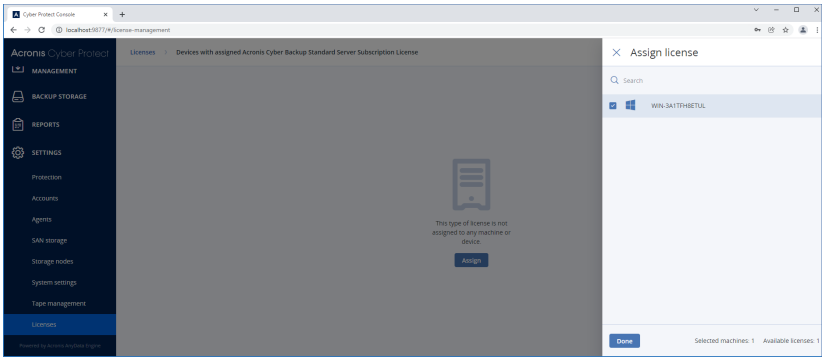
Aby przypisać licencję subskrypcyjną do obciążenia

1. W konsoli internetowej Cyber Protect przejdź do sekcji **Ustawienia** > **Licencje**.
2. Przejdź do odpowiedniej licencji i kliknij **Zarządzaj**.



3. Kliknij **Przypisz**.

   Zostaną wyświetlone obciążenia, do których można przypisać tę licencję.



4. Wybierz obciążenie i kliknij **Gotowe**.

Aby odwołać licencję subskrypcyjną z obciążenia

1. W konsoli internetowej Cyber Protect przejdź do sekcji **Ustawienia** > **Licencje**.
2. Przejdź do odpowiedniej licencji i kliknij **Zarządzaj**.

   Zostaną wyświetlone wszystkie obciążenia, do których jest przypisana ta licencja.
3. Wybierz obciążenie, z którego chcesz odwołać licencję.
4. Kliknij **Odwołaj**.
5. Potwierdź decyzję.

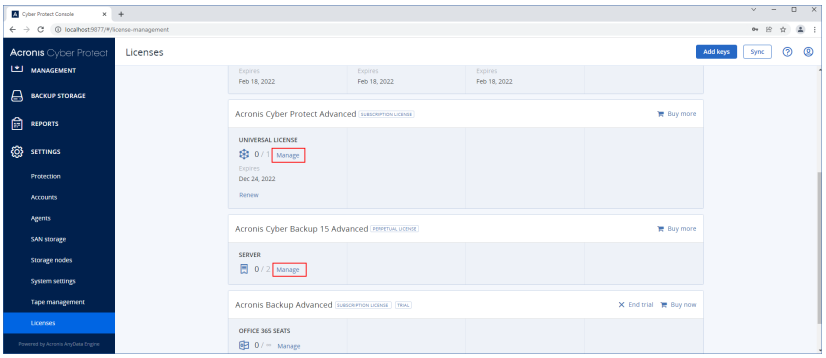
   Odwołana licencja zostanie zwolniona i będzie można ją przypisać do innego obciążenia.

Zarządzanie licencjami wieczystymi

Przed przypisaniem licencji do obciążenia trzeba dodać klucz licencyjny do serwera zarządzania. Dodatkowe informacje na ten temat można znaleźć w sekcji "Dodawanie kluczy licencyjnych do serwera zarządzania" (s. 42).

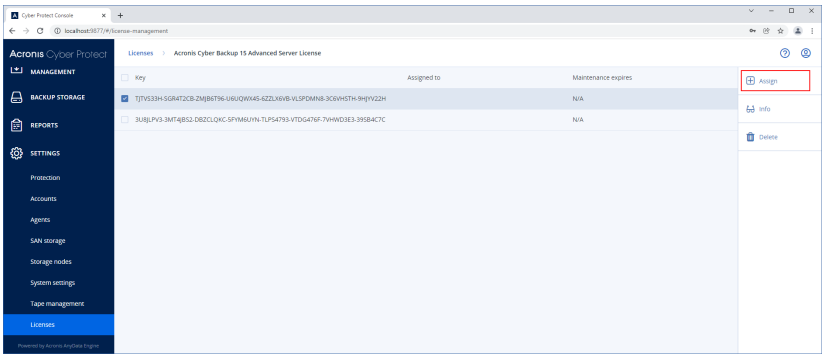
Aby przypisać licencję wieczystą do obciążenia

1. W konsoli internetowej Cyber Protect przejdź do sekcji **Ustawienia** > **Licencje**.
2. Przejdź do odpowiedniej licencji i kliknij **Zarządzaj**.



Zostaną wyświetlone klucze licencyjne odpowiadające wybranej licencji.

3. Wybierz klucz licencyjny, który chcesz przypisać do obciążenia.
4. Kliknij **Przypisz**.



Zostaną wyświetlone obciążenia, do których można przypisać ten klucz licencyjny.

5. Wybierz obciążenie i kliknij **Gotowe**.

Aby odwołać licencję wieczystą z obciążenia

1. W konsoli internetowej Cyber Protect przejdź do sekcji **Ustawienia** > **Licencje**.
2. Wybierz odpowiednią licencję i kliknij **Zarządzaj**.

   Zostaną wyświetlone klucze licencyjne odpowiadające wybranej licencji. W kolumnie **Przypisano do** sprawdź obciążenie, do którego jest przypisany ten klucz licencyjny.
3. Wybierz klucz licencyjny, który chcesz odwołać.
4. Kliknij **Odwołaj**.
5. Potwierdź decyzję.

   Odwołany klucz licencyjny pozostaje na liście licencji i można go przypisać do innego obciążenia.

Instalacja

Omówienie instalacji

Program Acronis Cyber Protect obsługuje dwie metody wdrożeń: lokalne oraz chmurowe. Metody te różnią się przede wszystkim lokalizacją serwera zarządzania Acronis Cyber Protect.

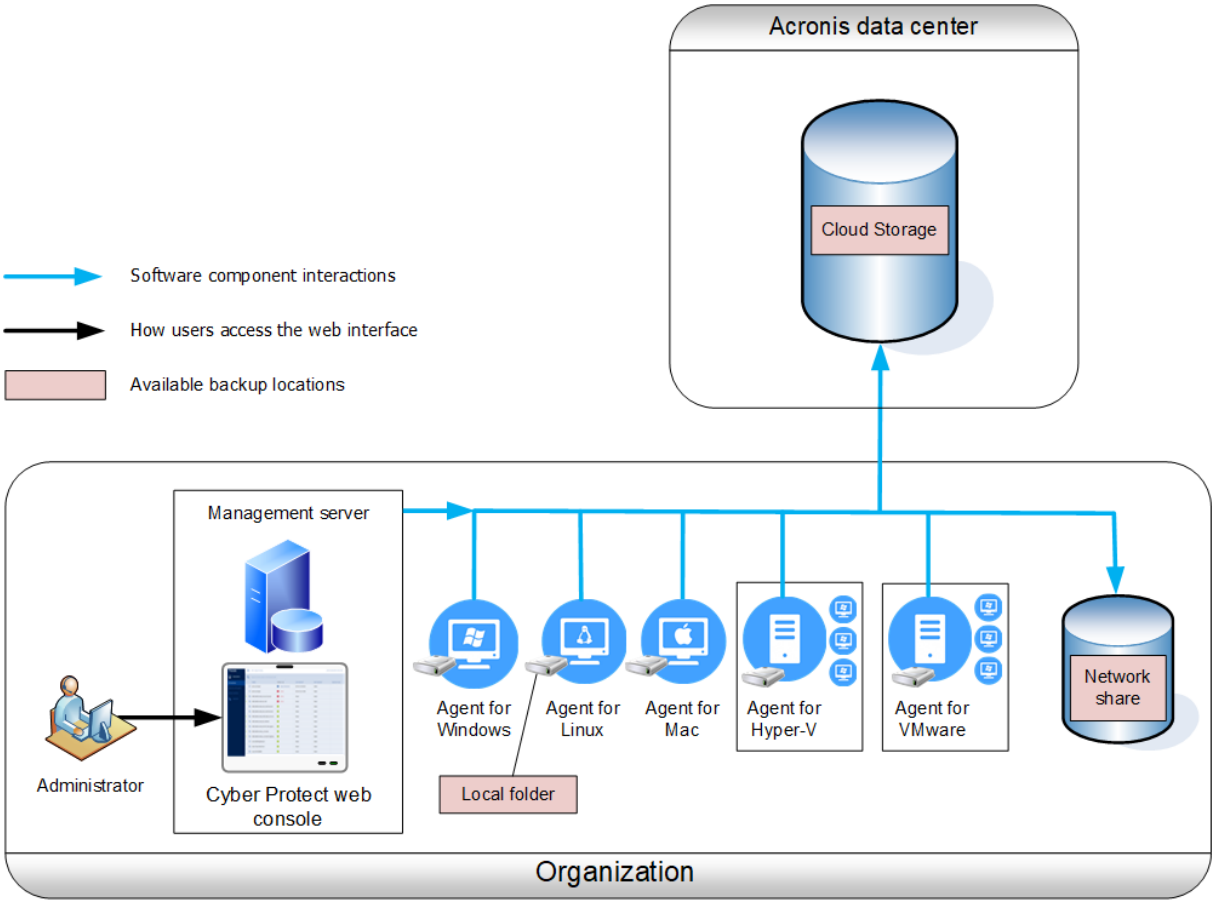
Serwer zarządzania stanowi centralny punkt zarządzania wszystkimi kopiami zapasowymi. W przypadku wdrożenia lokalnego jest on zainstalowany w sieci lokalnej, natomiast w przypadku wdrożenia chmurowego znajduje się w jednym z centrów danych firmy Acronis. Interfejs internetowy tego serwera jest nazywany konsolą internetową Cyber Protect.

Serwer zarządzania odpowiada za komunikację z agentami ochrony i ogólne funkcje z zakresu zarządzania planami. Przed podjęciem jakiegokolwiek działania w ramach ochrony agenty komunikują się z serwerem zarządzania w celu weryfikacji warunków wstępnych. Czasem połączenie z serwerem zarządzania może zostać utracone, co uniemożliwia wdrożenie nowych planów ochrony. Jeśli jednak na komputerze został już wdrożony plan ochrony, agent kontynuuje operacje związane z ochroną przez 30 dni od utraty komunikacji z serwerem zarządzania.

Oba rodzaje wdrożeń wymagają instalacji agenta ochrony na każdym komputerze, którego kopię zapasową chcesz utworzyć. Obsługiwane są też takie same typy magazynów. Miejsce w chmurze jest do nabycia osobno od licencji programu Acronis Cyber Protect.

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.



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. Zaawansowana licencja pozwala tworzyć jednostki organizacyjne i dodawać do nich administratorów. W ten sposób możesz przekazać zarządzanie ochroną innym osobom, których uprawnienia dostępu będą ściśle ograniczone do odpowiednich jednostek.

Instalacja w systemie Linux jest zalecana w środowiskach opartych wyłącznie na systemie Linux. Agenta trzeba zainstalować lokalnie na komputerach, których kopie zapasowe chcesz utworzyć.

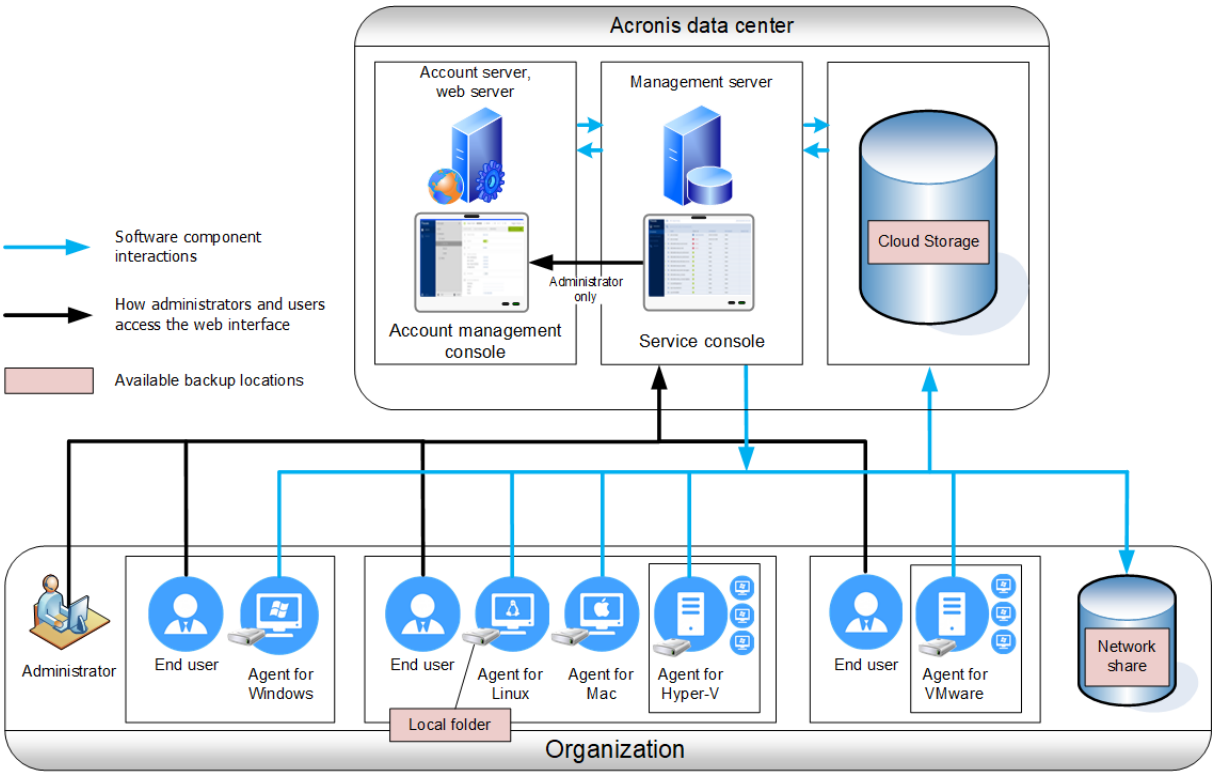
Wdrożenie chmurowe

Wdrożenie chmurowe oznacza, że serwer zarządzania znajduje się w jednym z centrów danych firmy Acronis. Zaletą tego rozwiązania jest brak konieczności konserwacji serwera zarządzania w sieci lokalnej. Acronis Cyber Protect można w tym przypadku uznać za usługę ochrony cybernetycznej udostępnianą 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 otworzyć konsolę internetową Cyber Protect, 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 przedstawiono różnice między wdrożeniem lokalnym a wdrożeniem w chmurze. Poszczególne kolumny zawierają listy funkcji dostępnych tylko w danym rodzaju wdrożenia.

Wdrożenie lokalne	Wdrożenie chmurowe
• Możliwość korzystania z licencji wieczystych • Lokalny serwer zarządzania, który może być używany w przypadku odseparowanych środowisk* • Serwer SFTP jako lokalizacja kopii zapasowych • Acronis Cyber Infrastructure jako lokalizacja kopii zapasowych • Urządzenia taśmowe i węzły Acronis Storage Node jako lokalizacje kopii zapasowych** • Uaktualnienie ze starszych wersji programu Acronis Cyber Protect, w tym Acronis Backup for VMware	• Tworzenie kopii zapasowych z chmury do chmury w przypadku danych usługi Microsoft 365, w tym ochrona grup, folderów publicznych oraz danych programów OneDrive*** i SharePoint Online • Tworzenie kopii zapasowej z chmury do chmury danych z Google Workspace • Agent dla systemu Mac obsługuje zarówno procesory x64, jak i ARM, takie jak Apple Silicon M1 i M2 • Agent dla Virtuozzo (tworzenie kopii zapasowych maszyn wirtualnych Virtuozzo na poziomie hiperwizora) • Agent dla oVirt (tworzenie kopii zapasowych maszyn wirtualnych oVirt KVM na poziomie

	hiperwizora) • Agent dla Virtuozzo Hybrid Infrastructure (tworzenie kopii zapasowych maszyn wirtualnych Virtuozzo Hybrid Infrastructure na poziomie hiperwizora) • Odzyskiwanie po awarii jako usługa chmurowa****

* Dodatkowe informacje na temat aktywowania serwera zarządzania w środowisku odseparowanym można znaleźć w sekcji "Aby aktywować serwer zarządzania offline" (s. 28).

** Funkcja niedostępna w wersji Standard.

***Folder główny OneDrive jest domyślnie wykluczany z operacji tworzenia kopii zapasowych. W przypadku wybrania określonych plików i folderów OneDrive będą one uwzględniane w kopii zapasowej. Pliki, które nie są dostępne na urządzeniu, będą miały nieprawidłową zawartość w archiwum.

**** Funkcja dostępna tylko z dodatkiem Odzyskiwanie po awarii.

Komponenty

Agenty

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

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

Niektóre agenty mogą zostać zainstalowane tylko na komputerach z określonymi rolami lub aplikacjami, na przykład agent dla Hyper-V jest instalowany na komputerach z rolą Hyper-V, agent dla SQL — na komputerach z bazami danych SQL, agent dla programu Exchange — na komputerach z rolą Skrzynka pocztowa programu Microsoft Exchange Server, a agent dla usługi Active Directory — na kontrolerach domen.

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

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 macOS	Agent dla systemu Mac		+	+
Aplikacje				
Bazy danych SQL	Agent dla SQL	Na komputerze z programem Microsoft SQL Server.	+	+
Bazy danych i skrzynki pocztowe programu Exchange	Agent dla programu Exchange	Na komputerze z rolą Skrzynka pocztowa programu Microsoft Exchange Server*. Jeśli jest wymagana tylko kopia zapasowa skrzynki pocztowej, agent może zostać zainstalowany na dowolnym komputerze z systemem Windows, który ma dostęp sieciowy do komputera z uruchomioną rolą Dostęp klienta programu Microsoft Exchange Server.	+	+ Brak kopii zapasowej skrzynki pocztowej
Skrzynki pocztowe Microsoft 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.	+	+
Komputery z systemem Oracle Database	Agent dla programu Oracle	Na komputerze z systemem Oracle Database.	+	-
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 Scale Computing HC3	Agent dla Scale Computing HC3	Na hoście Scale Computing HC3.	+	+
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			+	+
Maszyny wirtualne Citrix XenServer			+****	+
Maszyny wirtualne Red Hat Virtualization				

(RHV/RHEV)				
Maszyny wirtualne oparte na jądrze (KVM)				
Maszyny wirtualne Oracle				
Maszyny wirtualne Nutanix AHV				
Urządzenia mobilne				
Urządzenia mobilne z systemem Android	Aplikacja mobilna dla systemu Android	Na urządzeniu mobilnym, którego kopia zapasowa zostanie utworzona.	-	+
Urządzenia przenośne z systemem iOS	Aplikacja mobilna dla systemu iOS		-	+

* Podczas instalacji agent dla programu Exchange sprawdza, czy na komputerze, na którym będzie uruchamiany, jest wystarczająco dużo wolnego miejsca. Podczas odzyskiwania granularnego tymczasowo potrzeba wolnego miejsca na poziomie 15% największej bazy danych Exchange.

** 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 „Tworzenie kopii zapasowych bez obciążania sieci lokalnej”.

*** Maszyna wirtualna jest uznawana za wirtualną, jeśli jej kopie zapasowe są tworzone przez agenta zewnętrznego. 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.

**** W przypadku stosowania licencji hosta Acronis Cyber Protect Advanced Virtual Host te maszyny wirtualne są traktowane jak maszyny wirtualne (jest stosowane licencjonowanie na host). W przypadku licencji hosta Acronis Cyber Protect Virtual Host te maszyny wirtualne są traktowane jak komputery fizyczne (jest stosowane licencjonowanie na komputer).

Inne komponenty

Komponent	Funkcja	Gdzie trzeba go zainstalować?	Dostępność	
			Lokalnie	Chmura

Serwer zarządzania	Serwer zarządzania jest centralnym punktem zarządzania wszystkimi kopiami zapasowymi. W przypadku wdrożenia lokalnego jest on instalowany w sieci lokalnej. Zarządza agentami i udostępnia użytkownikom interfejs internetowy.	Na komputerze z systemem Windows lub Linux.	+	-
Komponenty do instalacji zdalnej	Zapisuje pakiety instalacyjne agentów w folderze lokalnym.	Na komputerze z systemem Windows i uruchomionym serwerem zarządzania.	+	-
Usługa Skanowanie	Komponent opcjonalny, który umożliwia skanowanie antywirusowe kopii zapasowych w chmurze, w folderze lokalnym lub w folderze sieciowym. Usługa Skanowanie wymaga bazy danych Microsoft SQL Server lub PostgreSQL. Nie jest ona zgodna z domyślną bazą danych SQLite używaną przez serwer zarządzania.	Na komputerze z systemem Windows lub Linux i uruchomionym serwerem zarządzania.	+	-
Generator nośnika startowego	Tworzy nośnik startowy.	Na komputerze z systemem Windows lub Linux.	+	-
Narzędzie wiersza polecenia	Obsługuje interfejs wiersza polecenia za pomocą programu	Na komputerze z systemem Windows, Linux lub macOS.	+	+

	narzędziowego **acrocmd**. Program **acrocmd** nie zawiera żadnych narzędzi fizycznie wykonujących polecenia. On jedynie udostępnia interfejs wiersza polecenia komponentom usługi Cyber Protect — agentom oraz serwerowi zarządzania.			
Acronis Cyber Protect 15 Monitor	Udostępnia graficzny interfejs użytkownika dla agenta dla systemu Windows i agenta dla systemu Mac. Są w nim wyświetlane informacje o statusie ochrony komputera, na którym zainstalowano agenta, a ponadto umożliwia skonfigurowanie ustawień szyfrowania kopii zapasowych i ustawień serwera proxy. W przypadku systemu Windows Acronis Cyber Protect 15 Monitor wymaga, aby na tym samym komputerze był zainstalowany agent dla systemu Windows.	Na komputerze z systemem Windows lub macOS.	+	+
Węzeł magazynowania	Przechowuje kopie zapasowe. Jest wymagany do	Na komputerze z systemem Windows.	+	-

	katalogowania i deduplikacji. Program Storage Node wymaga, aby na tym samym komputerze był zainstalowany agent dla systemu Windows.			
Usługa wykazu	Wykonuje katalogowanie kopii zapasowych na węzłach magazynowania.	Na komputerze z systemem Windows.	+	-
Serwer PXE	Umożliwia uruchamianie komputerów na nośnikach startowych przez sieć.	Na komputerze z systemem Windows.	+	-

Korzystanie z Acronis Cyber Protect z innymi rozwiązaniami z zakresu bezpieczeństwa w danym środowisku

Programu Acronis Cyber Protect można używać razem z innymi rozwiązaniami z zakresu bezpieczeństwa, np. autonomicznym programem antywirusowym, w jednym środowisku.

Jeśli nie dysponujesz innym rozwiązaniem z zakresu bezpieczeństwa, program Acronis Cyber Protect może zapewniać pełną ochronę cybernetyczną lub tradycyjne funkcje tworzenia kopii zapasowych i odzyskiwania — w zależności od licencji i stosownie do potrzeb. Dodatkowe informacje na temat funkcji dostępnych w ramach poszczególnych licencji można znaleźć w sekcji „Porównanie wersji programu Acronis Cyber Protect 15, w tym wdrożenia chmurowego”. Zakres planów ochrony można dostosować przez włączenie tylko potrzebnych modułów.

Wybierz opcję Acronis Cyber Protect, aby uzyskać pełną ochronę cybernetyczną, w tym ochronę przed wirusami i innym złośliwym oprogramowaniem, nawet jeśli w środowisku znajduje się już inne rozwiązanie z zakresu bezpieczeństwa. W takim przypadku należy wyłączyć lub usunąć to drugie rozwiązanie z zakresu bezpieczeństwa, aby uniknąć konfliktów.

Można też wzmocnić ochronę cybernetyczną bez wyłączania lub usuwania obecnego rozwiązania z zakresu bezpieczeństwa. To również jest możliwe — po prostu upewnij się, że nie używasz w

planach ochrony modułu Ochrona przed wirusami i złośliwym oprogramowaniem. Pozostałych modułów można swobodnie używać.

Ograniczenia

- Skanowanie antywirusowe kopii zapasowych wymaga zainstalowania usługi Skanowanie wraz z serwerem Cyber Protect Management Server.
- Połączenie przez klienta HTML5 jest dostępne tylko wtedy, gdy serwer Cyber Protect Management Server jest instalowany na komputerze z systemem Linux.

Wymagania dotyczące oprogramowania

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

Uwaga
W przypadku wdrożeń w chmurze przeglądarka Internet Explorer nie jest obsługiwana.

- Microsoft Edge 25 lub nowsza
- Safari 8 lub nowsza w systemach operacyjnych macOS 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.

Obsługiwane systemy operacyjne i środowiska

Agenty

Agent dla systemu Windows

- Windows XP Professional SP1 (x64), SP2 (x64), SP3 (x86)
- Windows XP Professional SP2 (x86) — obsługiwany przy użyciu specjalnej wersji agenta dla systemu Windows. Szczegółowe informacje i zestawienie ograniczeń obsługi zawiera sekcja „Agent dla systemu Windows XP SP2”.
- Windows XP Embedded SP3
- Windows Server 2003 SP1/2003 R2 lub nowszy — wersje Standard i Enterprise (x86, x64)

Uwaga

Program Acronis Cyber Protect wymaga aktualizacji KB940349 firmy Microsoft, której już nie można osobno pobrać. Aby na komputerze były dostępne funkcje zapewniane wcześniej przez aktualizację KB940349, należy zainstalować wszystkie aktualnie dostępne aktualizacje dla systemu Windows Server 2003.

Dodatkowe informacje na temat aktualizacji KB940349 można znaleźć w tym artykule z bazy wiedzy Knowledge Base.

- Windows Small Business Server 2003/2003 R2
- Windows Server 2008 — wersje Standard, Enterprise, Datacenter, Foundation i Web (x86, x64)
- Windows Small Business Server 2008
- Windows 7 — wszystkie wersje (x86, x64)

Uwaga

Aby korzystać z rozwiązania Acronis Cyber Protect w połączeniu z systemem Windows 7, trzeba zainstalować następujące aktualizacje z firmy Microsoft:

- Rozszerzone aktualizacje zabezpieczeń (ESU) systemu Windows 7
- KB4474419
- KB4490628

Więcej informacji na temat wymaganych aktualizacji można znaleźć w tym artykule bazy wiedzy Knowledge Base.

- Windows Server 2008 R2 — wersje Standard, Enterprise, Datacenter, Foundation i Web
- Windows Home Server 2011
- Windows MultiPoint Server 2010/2011/2012
- Windows Small Business Server 2011 — wszystkie wersje
- Windows 8/8.1 — wszystkie wersje (x86, x64) z wyjątkiem systemu Windows RT
- Windows Server 2012/2012 R2 — wszystkie wersje
- Windows Storage Server 2003/2008/2008 R2/2012/2012 R2/2016
- Windows 10 — wersje Home, Pro, Education, Enterprise, IoT Enterprise i LTSC (dawniej LTSB)
- Windows Server 2016 — wszystkie opcje instalacji z wyjątkiem systemu Nano Server
- Windows Server 2019 — wszystkie opcje instalacji z wyjątkiem systemu Nano Server
- Windows 11 — wszystkie wersje
- Windows Server 2022 — wszystkie opcje instalacji z wyjątkiem systemu Nano Server

Agent dla SQL, agent dla programu Exchange (na potrzeby kopii zapasowych baz danych oraz kopii zapasowych uwzględniających aplikacje), agent dla usługi Active Directory

Każdy z tych agentów można zainstalować na komputerze z dowolnym wymienionym wyżej systemem operacyjnym i obsługiwaną wersją odpowiedniej aplikacji, z następującym wyjątkiem:

- Agent dla SQL nie jest obsługiwany w przypadku wdrożeń lokalnych w systemach Windows 7 Starter oraz Home (x86, x64)

Agent dla programu Exchange (na potrzeby kopii zapasowych skrzynek pocztowych)

Tego agenta można zainstalować na komputerze z programem Microsoft Exchange Server lub bez tego programu.

- Windows Server 2008 — wersje Standard, Enterprise, Datacenter, Foundation 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
- Windows Small Business Server 2011 — wszystkie wersje
- Windows 8/8.1 — wszystkie wersje (x86, x64) z wyjątkiem systemu Windows RT
- 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
- Windows Server 2019 — wszystkie opcje instalacji z wyjątkiem systemu Nano Server
- Windows 11 — wszystkie wersje
- Windows Server 2022 — wszystkie opcje instalacji z wyjątkiem systemu Nano Server

Agent dla usługi Office 365

- Windows Server 2008 — wersje Standard, Enterprise, Datacenter, Foundation i Web (tylko x64)
- Windows Small Business Server 2008
- Windows Server 2008 R2 — wersje Standard, Enterprise, Datacenter, Foundation i Web
- Windows Home Server 2011
- Windows Small Business Server 2011 — wszystkie wersje
- Windows 8/8.1 — wszystkie wersje (tylko 64-bitowe) oprócz Windows RT
- Windows Server 2012/2012 R2 — wszystkie wersje

- Windows Storage Server 2008/2008 R2/2012/2012 R2/2016 (tylko wersje x64)
- Windows 10 — wersje Home, Pro, Education i Enterprise (tylko x64)
- Windows Server 2016 — wszystkie opcje instalacji (tylko x64) z wyjątkiem serwera Nano Server
- Windows Server 2019 — wszystkie opcje instalacji (tylko x64) z wyjątkiem serwera Nano Server
- Windows 11 — wszystkie wersje
- Windows Server 2022 — wszystkie opcje instalacji z wyjątkiem systemu Nano Server

Agent dla programu Oracle

- Windows Server 2008 R2 — wersje Standard, Enterprise, Datacenter i Web (x86, x64)
- Windows Server 2012 R2 — wersje Standard, Enterprise, Datacenter i Web (x86, x64)
- Linux — dowolne jądro i dowolna dystrybucja obsługiwane przez agenta dla systemu Linux (wymieniono niżej)

Agent dla systemu Linux

Uwaga
Poniższe dystrybucje i wersje jądra systemu Linux zostały specjalnie przetestowane. Ale nawet jeśli dana dystrybucja lub wersja jądra systemu Linux nie jest niżej wymieniona, to ze względu na specyfikę systemów operacyjnych Linux może wciąż poprawnie działać we wszystkich wymaganych zastosowaniach.

Jeśli w przypadku korzystania z programu Acronis Cyber Protect w połączeniu z daną dystrybucją i wersją jądra systemu Linux wystąpią problemy, skontaktuj się z zespołem pomocy technicznej w celu przeprowadzenia dokładniejszego dochodzenia.

Linux z jądrem w wersjach od 2.6.9 do 5.19 i biblioteką glibc w wersji 2.3.4 lub nowszą, w tym następujące dystrybucje x86 i x86_64:

- Red Hat Enterprise Linux 4.x, 5.x, 6.x, 7.x, 8.0, 8.1, 8.2, 8.3, 8.4*, 8.5*, 8.6*, 8.7*
- 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, 16.10, 17.04, 17.10, 18.04, 18.10, 19.04, 19.10, 20.04, 20.10, 21.04, 21.10, 22.04
- Fedora 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31
- SUSE Linux Enterprise Server 10, 11, 12, 15

  Ważne
  W przypadku systemów SUSE Linux Enterprise Server 12 i SUSE Linux Enterprise Server 15 nie są obsługiwane konfiguracje z systemem plików Btrfs.

- Debian 4.x, 5.x, 6.x, 7.0, 7.2, 7.4, 7.5, 7.6, 7.7, 8.0, 8.1, 8.2, 8.3, 8.4, 8.5, 8.6, 8.7, 8.8, 8.11, 9.0, 9.1, 9.2, 9.3, 9.4, 9.5, 9.6, 9.7, 9.8, 10, 11
- CentOS 5.x, 6.x, 7.x, 8.0, 8.1, 8.2, 8.3, 8.4*, 8.5*

- CentOS Stream 8
- Oracle Linux 5.x, 6.x, 7.x, 8.0, 8.1, 8.2, 8.3, 8.4*, 8.5*– wersje Unbreakable Enterprise Kernel i Red Hat Compatible Kernel
- CloudLinux 5.x, 6.x, 7.x, 8.0, 8.1, 8.2, 8.3, 8.4*, 8.5*
- ClearOS 5.x, 6.x, 7.x, 8.0, 8.1, 8.2, 8.3, 8.4*, 8.5*
- AlmaLinux 8.4*, 8.5*
- Rocky Linux 8.4*
- ALT Linux 7.0

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

Jeśli używana dystrybucja systemu Linux nie obsługuje mechanizmu D-Bus (na przykład Red Hat Enterprise Linux 6.x lub CentOS 6.x), program Acronis Cyber Protect użyje domyślnej lokalizacji w celu zapisania bezpiecznych kluczy, ponieważ system operacyjny nie zapewnia lokalizacji zgodnej z mechanizmem D-Bus.

* Obsługiwane tylko w przypadku jąder w wersjach od 4.18 do 5.19

Agent dla systemu Mac

Uwaga
Procesory oparte na architekturze ARM, takie jak Apple Silicon M1 i M2, nie są obsługiwane.

- OS X Mavericks 10.9
- OS X Yosemite 10.10
- OS X El Capitan 10.11
- macOS Sierra 10.12
- macOS High Sierra 10.13
- macOS Mojave 10.14
- macOS Catalina 10.15
- macOS Big Sur 11
- macOS Monterey 12
- macOS Ventura 13

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, 6.5, 6.7, 7.0, 8.0

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 (tylko x64) z rolą Hyper-V, w tym tryb instalacji Server Core
- Windows Server 2008 R2 z rolą Hyper-V, w tym tryb instalacji Server Core
- Microsoft Hyper-V Server 2008/2008 R2
- Windows Server 2012/2012 R2 z rolą Hyper-V, w tym tryb instalacji Server Core
- Microsoft Hyper-V Server 2012/2012 R2
- Windows 8, 8.1 (tylko 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
- Windows Server 2019 z rolą Hyper-V — wszystkie opcje instalacji z wyjątkiem systemu Nano Server
- Microsoft Hyper-V Server 2019
- Windows Server 2022 z rolą Hyper-V — wszystkie opcje instalacji, z wyjątkiem systemu Nano Server

Agent dla Scale Computing HC3 (urządzenie wirtualne)

Ten agent jest dostarczany jako urządzenie wirtualne wdrażane w klastrze Scale Computing HC3 za pośrednictwem konsoli internetowej Cyber Protect. W jego przypadku nie ma osobnego instalatora.

Scale Computing Hypercore 8.8, 8.9, 9.0

Serwer zarządzania (tylko w ramach wdrożenia lokalnego)

W systemie Windows

- Windows 7 — wszystkie wersje (x86, x64)

  Uwaga
  Aby korzystać z rozwiązania Acronis Cyber Protect w połączeniu z systemem Windows 7, trzeba zainstalować następujące aktualizacje z firmy Microsoft:
  - Rozszerzone aktualizacje zabezpieczeń (ESU) systemu Windows 7
  - KB4474419
  - KB4490628

  Więcej informacji na temat wymaganych aktualizacji można znaleźć w tym artykule bazy wiedzy Knowledge Base.

- Windows Server 2008 R2 — wersje Standard, Enterprise, Datacenter i Foundation
- Windows Home Server 2011
- Windows MultiPoint Server 2010/2011/2012
- Windows Small Business Server 2011 — wszystkie wersje
- Windows 8/8.1 — wszystkie wersje (x86, x64) z wyjątkiem systemu Windows RT
- Windows Server 2012/2012 R2 — wszystkie wersje
- Windows Storage Server 2008 R2 / 2012 / 2012 R2 / 2016
- Windows 10 — wersje Home, Pro, Education, Enterprise, IoT Enterprise i LTSC (dawniej LTSB)
- Windows Server 2016 — wszystkie opcje instalacji z wyjątkiem systemu Nano Server
- Windows Server 2019 — wszystkie opcje instalacji z wyjątkiem systemu Nano Server
- Windows 11 — wszystkie wersje
- Windows Server 2022 — wszystkie opcje instalacji z wyjątkiem systemu Nano Server

W systemie Linux

Uwaga
Poniższe dystrybucje i wersje jądra systemu Linux zostały specjalnie przetestowane. Ale nawet jeśli dana dystrybucja lub wersja jądra systemu Linux nie jest niżej wymieniona, to ze względu na specyfikę systemów operacyjnych Linux może wciąż poprawnie działać we wszystkich wymaganych zastosowaniach.

Jeśli w przypadku korzystania z programu Acronis Cyber Protect w połączeniu z daną dystrybucją i wersją jądra systemu Linux wystąpią problemy, skontaktuj się z zespołem pomocy technicznej w celu przeprowadzenia dokładniejszego dochodzenia.

Linux z jądrem w wersjach od 2.6.9 do 5.19 i biblioteką glibc w wersji 2.3.4 lub nowszą, w tym poniższe dystrybucje x86_64.

Dystrybucje x86 nie są obsługiwane.

- Red Hat Enterprise Linux 6.x, 7.x, 8.0, 8.1, 8.2, 8.3, 8.4*, 8.5*, 8.6*, 8.7*
- 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, 16.10, 17.04, 17.10, 18.04, 18.10, 19.04, 19.10, 20.04, 20.10, 21.04, 21.10, 22.04
- Fedora 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31
- SUSE Linux Enterprise Server 10, 11, 12, 15

Ważne
W przypadku systemów SUSE Linux Enterprise Server 12 i SUSE Linux Enterprise Server 15 nie są obsługiwane konfiguracje z systemem plików Btrfs.

- Debian 4.x, 5.x, 6.x, 7.0, 7.2, 7.4, 7.5, 7.6, 7.7, 8.0, 8.1, 8.2, 8.3, 8.4, 8.5, 8.6, 8.7, 8.8, 8.11, 9.0, 9.1, 9.2, 9.3, 9.4, 9.5, 9.6, 9.7, 9.8, 10, 11
- CentOS 5.x, 6.x, 7.x, 8.0, 8.1, 8.2, 8.3, 8.4*, 8.5*
- CentOS Stream 8
- Oracle Linux 5.x, 6.x, 7.x, 8.0, 8.1, 8.2, 8.3, 8.4*, 8.5*– wersje Unbreakable Enterprise Kernel i Red Hat Compatible Kernel
- CloudLinux 5.x, 6.x, 7.x, 8.0, 8.1, 8.2, 8.3, 8.4*, 8.5*
- ClearOS 5.x, 6.x, 7.x, 8.0, 8.1, 8.2, 8.3, 8.4*, 8.5*
- AlmaLinux 8.4*, 8.5*
- Rocky Linux 8.4*
- ALT Linux 7.0

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

Jeśli używana dystrybucja systemu Linux nie obsługuje mechanizmu D-Bus (na przykład Red Hat Enterprise Linux 6.x lub CentOS 6.x), program Acronis Cyber Protect użyje domyślnej lokalizacji w celu zapisania bezpiecznych kluczy, ponieważ system operacyjny nie zapewnia lokalizacji zgodnej z mechanizmem D-Bus.

* Obsługiwane tylko w przypadku jąder w wersjach od 4.18 do 5.19

Węzeł magazynowania (tylko na potrzeby wdrożenia lokalnego)

- Windows Server 2008 — wersje Standard, Enterprise, Datacenter i Foundation (tylko x64)
- Windows Small Business Server 2008
- Windows 7 — wszystkie wersje (tylko 64-bitowe)

- Windows Server 2008 R2 — wersje Standard, Enterprise, Datacenter i Foundation
- Windows Home Server 2011
- Windows MultiPoint Server 2010/2011/2012
- Windows Small Business Server 2011 — wszystkie wersje
- Windows 8/8.1 — wszystkie wersje (tylko 64-bitowe) oprócz Windows RT
- Windows Server 2012/2012 R2 — wszystkie wersje
- Windows Storage Server 2008 / 2008 R2 / 2012 / 2012 R2 / 2016
- Windows 10 — wersje Home, Pro, Education i IoT Enterprise
- Windows Server 2016 — wszystkie opcje instalacji z wyjątkiem systemu Nano Server
- Windows Server 2019 — wszystkie opcje instalacji z wyjątkiem systemu Nano Server
- Windows Server 2022 — wszystkie opcje instalacji z wyjątkiem systemu Nano Server

Agent dla systemu Windows XP SP2

Agent dla systemu Windows XP SP2 obsługuje tylko 32-bitową wersję systemu Windows XP SP2.

Aby chronić komputery z systemem Windows XP SP1 (x64), Windows XP SP2 (x64) lub Windows XP SP3 (x86), użyj zwykłego agenta dla systemu Windows.

Agent dla systemu Windows XP SP2 wymaga licencji Acronis Cyber Backup 12.5. Klucze licencyjne Acronis Cyber Protect 15 nie są obsługiwane.

Instalacja

Agent dla systemu Windows XP SP2 wymaga co najmniej 550 MB miejsca na dysku i 150 MB pamięci RAM. Podczas tworzenia kopii zapasowej agent używa zwykle około 350 MB pamięci. Wykorzystanie pamięci może sięgać 2 GB, zależnie od ilości przetwarzanych danych.

Agenta dla systemu Windows XP SP2 można zainstalować tylko lokalnie na komputerze, którego kopię zapasową chce się utworzyć. Aby pobrać program instalacyjny agenta, kliknij ikonę konta w prawym górnym rogu, a następnie kliknij **Do pobrania** > **Agent dla systemu Windows XP SP2**.

Nie można zainstalować narzędzia Cyber Protect Monitor ani Bootable Media Builder. Aby pobrać plik ISO nośnika startowego, kliknij ikonę konta w prawym górnym rogu > **Do pobrania** > **Nośnik startowy**.

Aktualizuj

Agent dla systemu Windows XP SP2 nie obsługuje funkcji aktualizacji zdalnej. Aby zaktualizować agenta, pobierz nową wersję programu instalacyjnego i jeszcze raz przeprowadź instalację.

Jeśli system Windows XP SP2 został zaktualizowany do wersji z dodatkiem SP3, odinstaluj agenta dla systemu Windows XP SP2, a następnie zainstaluj zwykłego agenta dla systemu Windows.

Ograniczenia

- Dostępne jest tylko tworzenie kopii zapasowych na poziomie dysku. Poszczególne pliki można odzyskiwać z kopii zapasowej dysku lub woluminu.
- Planowanie według zdarzeń nie jest obsługiwane.
- Warunki wykonania planu ochrony nie są obsługiwane.
- Obsługiwane są tylko następujące docelowe lokalizacje kopii zapasowych:
  - Chmura
  - Folder lokalny
  - Folder sieciowy
  - Secure Zone
- Format kopii zapasowej **Wersja 12** oraz funkcje wymagające formatu **Wersja 12** nie są obsługiwane. Przede wszystkim nie jest dostępne fizyczne dostarczanie danych. Opcja **Wydajność i okno na utworzenie kopii zapasowej**, jeśli jest włączona, powoduje zastosowanie tylko ustawień na poziomie zielonym.
- W interfejsie internetowym nie jest obsługiwany wybór poszczególnych dysków/woluminów do odzyskania ani ręczne mapowanie dysków podczas odzyskiwania. Ta funkcja jest dostępna tylko w ramach nośnika startowego.
- Przetwarzanie danych poza hostem nie jest obsługiwane.
- Agent dla systemu Windows XP SP2 nie może wykonywać następujących operacji na kopiach zapasowych:
  - Konwertowanie kopii zapasowych na maszynę wirtualną
  - Montowanie woluminów z kopii zapasowej
  - Wyodrębnianie plików z kopii zapasowej
  - Eksportowanie i ręczne sprawdzanie poprawności kopii zapasowej.

  Operacje te można wykonywać za pomocą innego agenta.
- Kopii zapasowych utworzonych przez agenta dla systemu Windows XP SP2 nie można uruchamiać jako maszyny wirtualnej.

Obsługiwane wersje programu Microsoft SQL Server

- Microsoft SQL Server 2022
- Microsoft SQL Server 2019
- Microsoft SQL Server 2017
- Microsoft SQL Server 2016
- Microsoft SQL Server 2014
- Microsoft SQL Server 2012

Obsługiwane są też wersje oprogramowania SQL Server Express wyżej wymienionych wersji serwera SQL.

Obsługiwane wersje programu Microsoft Exchange Server

- Microsoft Exchange Server 2019 — wszystkie wersje.
- 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. Kopie zapasowe skrzynki pocztowej i odzyskiwanie granularne z kopii zapasowej bazy danych są obsługiwane od wersji z dodatkiem Service Pack 1 (SP1).
- Microsoft Exchange Server 2007 — wszystkie wersje, wszystkie dodatki Service Pack. Kopie zapasowe skrzynki pocztowej i odzyskiwanie granularne z kopii zapasowej bazy danych nie są obsługiwane.

Obsługiwane wersje programu Microsoft SharePoint

Program Acronis Cyber Protect 15 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.

Obsługiwane wersje systemu Oracle Database

- Oracle Database w wersji 11g, wszystkie wydania
- Oracle Database w wersji 12c, wszystkie wydania

Obsługiwane są tylko konfiguracje obejmujące jedną instancję.

Obsługiwane wersje platformy SAP HANA

Platforma HANA 2.0 SPS 03 zainstalowana w systemie RHEL 7.6 działającym na komputerze fizycznym lub maszynie wirtualnej VMware ESXi.

Ponieważ platforma SAP HANA nie obsługuje odzyskiwania kontenerów baz danych z wieloma dzierżawcami przy użyciu migawek pamięci masowej, rozwiązanie to obsługuje kontenery SAP HANA z bazy danych z tylko jednym dzierżawcą.

Obsługiwane platformy wirtualizacji

W poniższej tabeli zestawiono możliwości obsługi poszczególnych platform wirtualizacji.

Uwaga
Specjalnie przetestowano niżej wymienionych dostawców i wersje hiperwizorów, które można obsługiwać przy użyciu metody **Kopia zapasowa z systemu operacyjnego gościa**. Jednak nawet w przypadku korzystania z hiperwizora od innego dostawcy lub w innej wersji niż wymieniono poniżej metoda **Kopia zapasowa z systemu operacyjnego gościa** wciąż może prawidłowo działać we wszystkich wymaganych zastosowaniach.

W razie napotkania problemów podczas korzystania z programu Acronis Cyber Protect w połączeniu z hiperwizorem od określonego dostawcy i w określonej wersji skontaktuj się z zespołem pomocy technicznej w celu przeprowadzenia dokładniejszego dochodzenia.

Platforma	Tworzenie kopii zapasowych na poziomie hiperwizora (bezagentowe tworzenie kopii zapasowych)	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, 6.7, 7.0, 8.0 **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 serwerem 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 technologią 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 Windows Server 2019 z rolą Hyper-V — wszystkie opcje instalacji z wyjątkiem systemu Nano Server Microsoft Hyper-V Server 2019 Windows Server 2022 z rolą Hyper-V — wszystkie opcje instalacji, z wyjątkiem systemu Nano Server	+	+
Microsoft Virtual PC 2004 i 2007 Windows Virtual PC		+
Microsoft Virtual Server 2005		+
Scale Computing		
Scale Computing Hypercore 8.8, 8.9, 9.0	+	+
Citrix		
Citrix XenServer 4.1.5, 5.5, 5.6, 6.0, 6.1, 6.2, 6.5, 7.0, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6		Tylko w pełni zwirtualizowane maszyny-goście (HVM). Parawirtualne maszyny-goście (PV) nie są obsługiwane.
Red Hat i Linux		
Red Hat Enterprise Virtualization (RHEV) 2.2, 3.0, 3.1, 3.2, 3.3, 3.4, 3.5, 3.6		+

Red Hat Virtualization (RHV) 4.0, 4.1		
Red Hat Virtualization (zarządzany przez oVirt) 4.2, 4.3, 4.4 (dostępne tylko w przypadku wdrożenia chmurowego)	+	+
Maszyny wirtualne oparte na jądrze (KVM)		+
Maszyny wirtualne oparte na jądrze (KVM) zarządzane przez oVirt 4.3 działające w systemie Red Hat Enterprise Linux 7.6 bądź 7.7 lub CentOS 7.6 bądź 7.7 (dostępne tylko w przypadku wdrożenia chmurowego i w ramach licencji Advanced)	+	+
Maszyny wirtualne oparte na jądrze (KVM) zarządzane przez oVirt 4.4 działające w systemie Red Hat Enterprise Linux 8.x lub CentOS Stream 8.x (dostępne tylko w przypadku wdrożenia chmurowego i licencji Advanced)	+	+
Maszyny wirtualne oparte na jądrze (KVM) zarządzane przez oVirt 4.5 działające w systemie Red Hat Enterprise Linux 8.x lub CentOS Stream 8.x (dostępne tylko w przypadku wdrożenia chmurowego i licencji Advanced)	+	+
Parallels		
Parallels Workstation		+
Parallels Server 4 Bare Metal		+
Oracle		
Oracle VM Server 3.0, 3.3, 3.4		Tylko w pełni zwirtualizowane maszyny-goście (HVM). Parawirtualne maszyny-goście (PV) nie są obsługiwane.
Oracle VM VirtualBox 4.x		+
Nutanix		
Hiperwizor Nutanix Acropolis (AHV) w wersji od 20160925.x do 20180425.x		+
Virtuozzo (dostępne tylko w przypadku wdrożenia chmurowego)		

Virtuozzo 6.0.10, 6.0.11, 6.0.12	+	Tylko maszyny wirtualne. Kontenery nie są obsługiwane.
Virtuozzo 7.0.13, 7.0.14	Tylko kontenery ploop. Maszyny wirtualne nie są obsługiwane.	Tylko maszyny wirtualne. Kontenery nie są obsługiwane.
Virtuozzo Hybrid Server 7.5	+	Tylko maszyny wirtualne. Kontenery nie są obsługiwane.
Virtuozzo Hybrid Infrastructure (dostępne tylko w przypadku wdrożenia chmurowego)		
Virtuozzo Hybrid Infrastructure 3.5, 4.0, 4.5	+	+
Amazon		
Instancje środowiska Amazon EC2		+
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.

*** Obsługiwane są maszyny wirtualne Hyper-V działające w klastrze hiperkonwergentnym z rozwiązaniem Storage Spaces Direct (S2D). Rozwiązanie Storage Spaces Direct jest też obsługiwane jako magazyn kopii zapasowych.

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 ochrony. 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 ochrony. Aby utworzyć kopię zapasową tych dysków lub znajdujących się na nich danych, zainstaluj agenta w systemie operacyjnym-gościu.
- **Klastrowanie gości Hyper-V**

  Agent dla Hyper-V nie obsługuje tworzenia kopii zapasowych maszyn wirtualnych Hyper-V będących węzłami klastra awaryjnego systemu Windows Server. Migawka VSS na poziomie hosta może nawet tymczasowo odłączyć zewnętrzny dysk kworum od klastra. Aby utworzyć kopię zapasową tych maszyn, zainstaluj agenty w systemach operacyjnych-gościach.
- **Połączenie iSCSI w systemie-gościu**

  Agent dla VMware ani agent dla Hyper-V nie tworzy kopii zapasowych woluminów LUN podłączonych przez inicjator iSCSI działający w systemie operacyjnym-gościu. Ponieważ hiperwizory ESXi i Hyper-V nie rozpoznają takich woluminów, woluminy te nie są uwzględniane w migawkach na poziomie hiperwizora i są bez ostrzeżenia pomijane podczas tworzenia kopii zapasowej. Aby utworzyć kopię zapasową takich woluminów lub znajdujących się na nich danych, należy zainstalować agenta w systemie operacyjnym-gościu.
- **Komputery z systemem Linux zawierające woluminy logiczne (LVM)**

  W przypadku komputerów z systemem Linux zawierających woluminy logiczne agent dla VMware i agent dla Hyper-V nie obsługują następujących operacji:
  - Migracja komputera fizycznego na maszynę wirtualną i maszyny wirtualnej na komputer fizyczny. Aby utworzyć kopię zapasową i nośnik startowy na potrzeby odzyskiwania, należy użyć agenta dla systemu Linux lub nośnika startowego.
  - Uruchomienie maszyny wirtualnej z kopii zapasowej utworzonej za pomocą agenta dla systemu Linux lub nośnika startowego.
  - Przekonwertowanie kopii zapasowej utworzonej za pomocą agenta dla systemu Linux lub nośnika startowego na maszynę wirtualną.
- **Szyfrowane maszyny wirtualne** (wprowadzone w środowisku VMware vSphere 6.5)
  - Szyfrowane maszyny wirtualne są zapisywane w kopii zapasowej w stanie niezaszyfrowanym. Jeśli szyfrowanie ma znaczenie krytyczne, włącz szyfrowanie kopii zapasowych podczas tworzenia planu ochrony.
  - 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 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.
- **Kopie zapasowe konfiguracji ESXi** nie są obsługiwane w przypadku systemu VMware vSphere 7.0.

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.
- Biblioteki `libelf-dev`, `libelf-devel` lub `elfutils-libelf-devel` do budowy jąder od 4.15 i konfigurowanych za pomocą polecenia CONFIG_UNWINDER_ORC=y. W niektórych dystrybucjach, takich jak Fedora 28, konieczna jest instalacja odrębna z nagłówków jądra.

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 `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.
5. W systemach Red Hat Enterprise Linux, CentOS i Fedora uruchom następujące polecenie celem sprawdzenia, czy zainstalowano pakiet `elfutils-libelf-devel`:

   ```
   yum list installed | grep elfutils-libelf-devel
   ```

   Jeśli zostanie wyświetlona informacja o wersji biblioteki, oznacza to, że biblioteka jest zainstalowana.

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** **elfutils-libelf-devel**	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** **elfutils-libelf-devel**	Program instalacyjny automatycznie pobierze i zainstaluje pakiety.
	perl	Uruchom następujące polecenie: `yum install perl`

Ubuntu
Debian
	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`

SUSE Linux OpenSUSE	**kernel-source** **gcc** **make** **perl**	sudo zypper install kernel-source sudo zypper install gcc sudo zypper install make sudo zypper 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
```

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 wskazać w jednym poleceniu `rpm`. Zainstalowanie każdego z pakietów może wymagać instalacji dodatkowych pakietów wynikających z określonych zależności.

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
- CheckPoint Harmony Endpoint
- 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

Zdecydowanie zalecamy zainstalowanie oprogramowania szyfrującego przed rozpoczęciem instalacji agentów ochrony.

Sposób korzystania ze strefy Secure Zone

Strefa Secure Zone nie może być zaszyfrowana na poziomie dysku. Ze strefy Secure Zone można korzystać tylko następująco:

1. Zainstaluj oprogramowanie szyfrujące.
2. Zainstaluj agenta ochrony.
3. Utwórz strefę Secure Zone.
4. Wyklucz strefę Secure Zone podczas 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 i CheckPoint Harmony Endpoint

System można odzyskać przy użyciu funkcji odzyskiwania z ponownym uruchomieniem lub nośnikiem startowym.

Odzyskiwanie z ponownym uruchomieniem

Aby odzyskać zaszyfrowany system, wykonaj czynności opisane w sekcji "Odzyskiwanie komputera fizycznego" (s. 324).

Upewnij się, że są spełnione wymagania przedstawione w sekcji "Odzyskiwanie z ponownym uruchomieniem" (s. 331).

Uwaga
W przypadku woluminów zaszyfrowanych przy użyciu funkcji Bitlocker odzyskiwanie z ponownym uruchomieniem jest dostępne tylko na komputerach z systemem Windows 7 lub nowszym albo Windows Server 2008 R2 lub nowszym opartych na technologii UEFI. W przypadku woluminów zaszyfrowanych przy użyciu narzędzia CheckPoint odzyskiwanie z ponownym uruchomieniem jest dostępne tylko na komputerach z systemem Windows 10 lub Windows 11.

Odzyskiwanie z ponownym uruchomieniem nie jest dostępne na komputerach z systemem BIOS ani na komputerach z systemem Linux lub macOS.

Odzyskiwanie przy użyciu nośnika startowego

1. Uruchom komputer za pomocą nośnika startowego.
2. Odzyskaj system.

   Ważne
   Dane z kopii zapasowej są odzyskiwane jako niezaszyfrowane.

3. Ponownie uruchom odzyskany system.
4. Włącz oprogramowanie szyfrujące.

Jeśli musisz odzyskać tylko jedną z wielu partycji dysku, wykonaj operację odzyskiwania 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.

Kompatybilność z urządzeniami pamięci masowej Dell EMC Data Domain

Korzystając z programu Acronis Cyber Protect, można używać urządzeń Dell EMC Data Domain jako magazynów kopii zapasowych. Jest obsługiwana blokada przechowywania (Tryb nadzoru).

W przypadku włączenia blokady przechowywania należy dodać zmienną środowiskową `AR_RETENTION_LOCK_SUPPORT` na komputerze z agentem ochrony, który używa tego magazynu jako miejsca docelowego kopii zapasowej.

Uwaga
Urządzenia pamięci masowej Dell EMC Data Domain z włączoną blokadą przechowywania nie są obsługiwane przez agenta dla systemu Mac.

Aby dodać zmienną w systemie Windows

1. Zaloguj się jako administrator na komputerze lub maszynie wirtualnej z agentem ochrony.
2. W oknie **Panel sterowania**, wybierz kolejno **System i zabezpieczenia** > **System** > **Zaawansowane zabezpieczenia systemu**.
3. Na karcie **Zaawansowane** kliknij **Zmienne środowiskowe**.
4. W panelu **Zmienne systemowe** kliknij **Nowa**.
5. W oknie **Nowa zmienna systemowa** dodaj następującą nową zmienną:
   - Nazwa zmiennej: `AR_RETENTION_LOCK_SUPPORT`
   - Wartość zmiennej: `1`
6. Kliknij **OK**.
7. W oknie **Zmienne środowiskowe** kliknij **OK**.
8. Uruchom ponownie komputer.

Aby dodać zmienną w systemie Linux

1. Zaloguj się jako administrator na komputerze lub maszynie wirtualnej z agentem ochrony.
2. Przejdź do katalogu `/sbin`, a następnie otwórz plik `acronis_mms` do edycji.
3. Na wierszem `export LD_LIBRARY_PATH` dodaj następujący wiersz:

   ```
   export AR_RETENTION_LOCK_SUPPORT=1
   ```

4. Zapisz plik `acronis_mms`.
5. Uruchom ponownie komputer.

Aby dodać zmienną na urządzeniu wirtualnym

1. Zaloguj się jako administrator na komputerze lub maszynie wirtualnej z urządzeniem wirtualnym.
2. Przejdź do katalogu `/bin`, a następnie otwórz plik `autostart` do edycji.
3. Pod wierszem `export LD_LIBRARY_PATH` dodaj następujący wiersz:

   ```
   export AR_RETENTION_LOCK_SUPPORT=1
   ```

4. Zapisz plik `autostart`.
5. Uruchom ponownie komputer z urządzeniem wirtualnym.

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	Miejsce na dysku wymagane do instalacji	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	2,0 GB	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
Serwer zarządzania w systemie Linux	1,5 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	4,0 GB	340 MB
Węzeł magazynowania i agent dla systemu Windows • Tylko platforma 64-bitowa • Do używania deduplikacji wymagane jest minimum 8 GB pamięci RAM. Aby uzyskać więcej informacji, zobacz "Sprawdzone praktyki dotyczące deduplikacji" (s. 647).	1,1 GB	330 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.

Tworzenie kopii zapasowych dużych zestawów kopii zapasowych (od 600 GB wzwyż) wymaga około 1 GB pamięci RAM na 1 TB zestawu kopii zapasowych.

Uwaga
W przypadku tworzenia kopii zapasowych w ramach bardzo dużych zestawów kopii zapasowych (o wielkości co najmniej 4 TB) zużycie pamięci RAM może wzrosnąć.

W systemach x64 operacje z nośnikiem startowym i odzyskiwanie dysku z ponownym uruchomieniem wymagają co najmniej 2 GB pamięci.

Serwer zarządzania z jednym zarejestrowanym obciążeniem używa 200 MB pamięci. Obciążenie to chroniony zasób dowolnego typu, na przykład komputer fizyczny, maszyna wirtualna, skrzynka pocztowa lub instancja bazy danych. Każde dodatkowe obciążenie oznacza dodatkowe około 2 MB. Oznacza to, że serwer ze 100 zarejestrowanymi obciążeniami używa około 400 MB ponad to, czego używa system operacyjny i uruchomione aplikacje.

Można zarejestrować maksymalnie 900–1000 obciążeń. Ograniczenie to wynika z wbudowanej w serwer zarządzania bazy danych SQLite.

Aby znieść to ograniczenie, należy podczas instalacji serwera zarządzania określić zewnętrzną instancję programu Microsoft SQL Server. Korzystając z zewnętrznej bazy danych SQL, można zarejestrować na serwerze zarządzania — bez wyraźnego pogorszenia wydajności — nawet 8000 obciążeń. W przypadku 8000 zarejestrowanych obciążeń instancja programu SQL Server będzie używać około 8 GB pamięci RAM.

Aby zwiększyć wydajność tworzenia kopii zapasowych, można zarządzać obciążeniami w grupach liczących do 500 obciążeń.

Obsługiwane systemy plików

Agent ochrony może tworzyć kopie zapasowe każdego systemu plików dostępnego 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.

System plików	Obsługujące agenty i nośniki				Ograniczenia
	Agenty	Przy użyciu nośnika startowego ze środowiskiem WinPE	Nośnik startowy oparty na systemie Linux	Nośnik startowy systemu Mac	
FAT16/32	Wszystkie agenty	+	+	+	Brak ograniczeń
NTFS		+	+	+	
ext2/ext3/ext4		+	+	-	
HFS+	Agent dla systemu Mac	-	-	+	
APFS		-	-	+	• Obsługiwany od wersji macOS High Sierra 10.13 • W przypadku odzyskiwania na komputer inny niż oryginalny lub komputer bez systemu operacyjnego należy ręcznie odtworzyć konfigurację dysków.

JFS	Agent dla systemu Linux	-	+	-	• Nie można wykluczać plików z kopii zapasowej dysku • Nie można włączyć opcji tworzenia szybkiej przyrostowej/różnicowej kopii zapasowej
ReiserFS3		-	+	-	
ReiserFS4		-	+	-	• Nie można wykluczać plików z kopii zapasowej dysku • Nie można włączyć opcji tworzenia szybkiej przyrostowej/różnicowej kopii zapasowej • Podczas odzyskiwania nie można zmieniać rozmiarów woluminów

ReFS	Wszystkie agenty	+	+	+	
XFS		+	+	+	• Nie można wykluczać plików z kopii zapasowej dysku • Nie można włączyć opcji tworzenia szybkiej przyrostowej/różnicowej kopii zapasowej • Podczas odzyskiwania nie można zmieniać rozmiarów woluminów • Odzyskiwanie plików z kopii zapasowej zapisanej na taśmie nie jest obsługiwane
Linux Swap	Agent dla systemu Linux	-	+	-	Brak ograniczeń
exFAT	Wszystkie agenty	+	+ Jeśli kopia zapasowa *jest przechowywana* w systemie plików exFAT, nie można przeprowadzić	+	• Obsługiwana jest wyłącznie kopia zapasowa dysku/woluminu • Nie można wykluczać plików z kopii zapasowej • Nie można odzyskiwać poszczególnych plików z kopii

			odzyskiwania przy użyciu nośnika startowego		zapasowej

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.

Deduplikacja danych

W systemie Windows Server 2012 lub nowszym można włączyć funkcję deduplikacji danych w przypadku woluminu NTFS. Deduplikacja danych zmniejsza ilość zużytego miejsca na woluminie dzięki jednokrotnemu zapisywaniu zduplikowanych na woluminie fragmentów plików.

W przypadku woluminów z włączoną funkcją deduplikacji danych można bez ograniczeń używać funkcji tworzenia kopii zapasowych na poziomie dysku oraz ich odzyskiwania. Tworzenie kopii zapasowych na poziomie plików jest obsługiwane, z wyjątkiem środowisk, w których jest używany dostawca Acronis VSS Provider. Aby odzyskać pliki z kopii zapasowej dysku, uruchom maszynę wirtualną z kopii zapasowej lub zamontuj kopię zapasową na komputerze z systemem operacyjnym Windows Server 2012 lub nowszym, a następnie skopiuj pliki z zamontowanego woluminu.

Funkcja deduplikacji danych systemu Windows Server nie jest związana z funkcją Acronis Backup Deduplication.

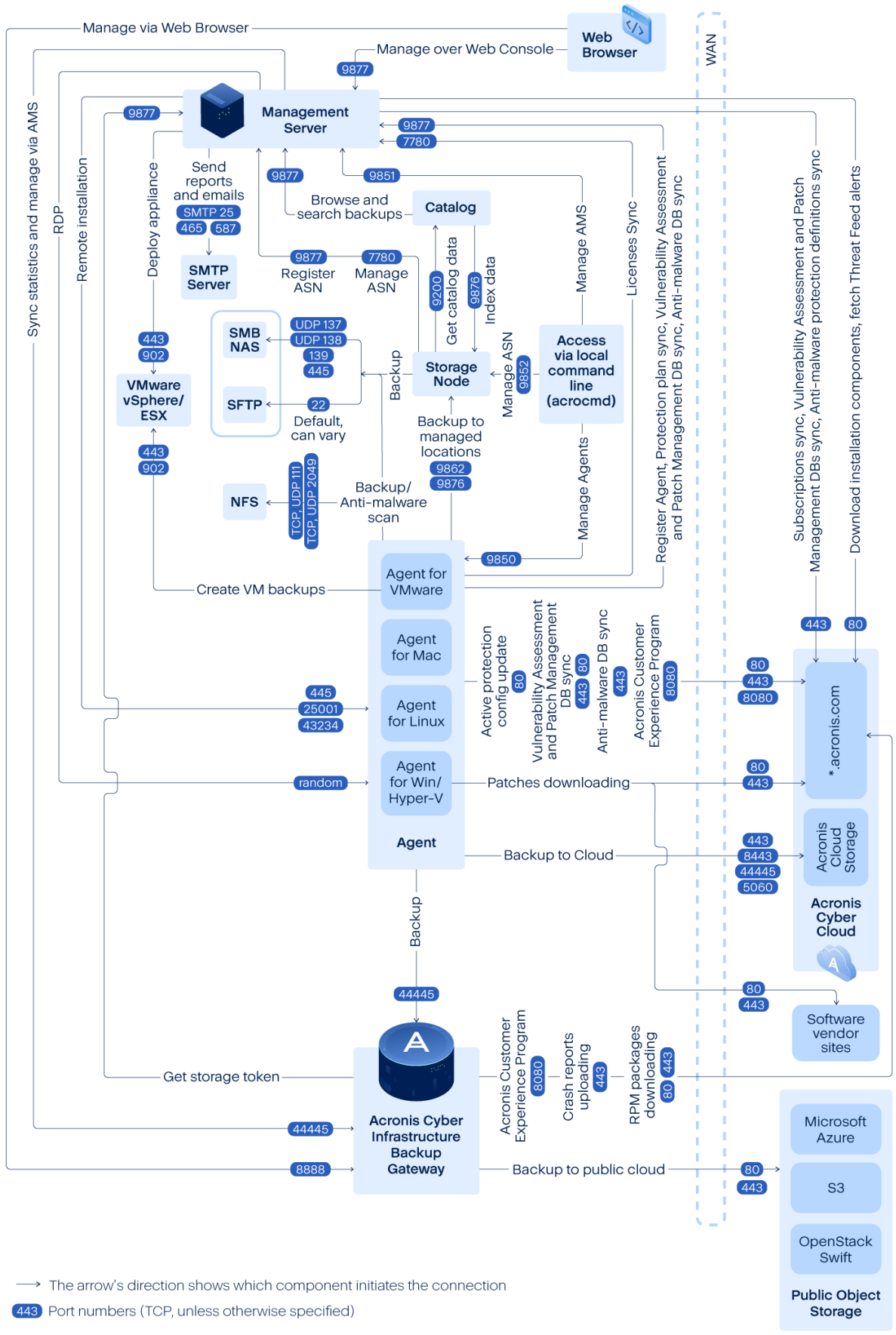
Diagram połączenia sieciowego dla Acronis Cyber Protect

Ten temat zawiera diagramy połączeń dla programu Acronis Cyber Protect.

Listę portów, usług i procesów, z których korzysta program Acronis Cyber Protect, można znaleźć w naszej bazie wiedzy Knowledge Base:

- W przypadku systemu Windows zobacz artykuł Windows services and processes (65663) (Usługi i procesy systemu Windows (65663)).
- W przypadku systemu Linux zobacz artykuł Linux components, services, and processes (67276) (Komponenty, usługi i procesy systemu Linux (67276)).

Diagram połączenia sieciowego — procesy Cyber Protect



Ważne
Porty wychodzące na diagramie sieci są dynamiczne. Niektóre usługi również mogą używać portów dynamicznych na potrzeby połączeń przychodzących. Podczas rozwiązywania problemów z siecią należy się upewnić, że jest dozwolony ruch przez porty dynamiczne.

Porty dynamiczne są zarządzane przez system operacyjny i przypisywane losowo. W systemie Windows domyślny zakres portów dynamicznych to 49152–65535. Zakres ten może być inny, w zależności od systemu operacyjnego — i można go zmienić ręcznie.

Serwer zarządzania jest centralnym składnikiem rozwiązania Acronis Cyber Protect. Udostępnia on dwa porty TCP: 7780 i 9877. Port 9877, chroniony przez protokół TLS, służy do udostępniania zarówno interfejsu REST API, jak i interfejsu użytkownika WWW. Punkty końcowe interfejsu REST API uwierzytelniają żądania za pomocą tokenów JWT reprezentowanych jako osobny nagłówek HTTP albo zakodowanych jako plik cookie HTTP. Port 7780 implementuje protokół ZeroMQ z uwierzytelnianiem i szyfrowaniem ZMTP CURVE. Port 7780 jest używany przez agenty i węzeł magazynowania do asynchronicznego wymieniania się z serwerem zarządzania komunikatami dotyczącymi zarządzania. Serwer zarządzania komunikuje się też z usługami w chmurze w celu pobierania aktualizacji przez standardowe porty HTTP i HTTPS.

Węzeł magazynowania jest komponentem magazynowym rozwiązania Acronis Cyber Protect. Udostępnia on port TCP 9876. Port ten służy do wysyłania i odbierania danych kopii zapasowych. Transport jest chroniony za pomocą protokołu TLS, a do uwierzytelniania jest używana technologia uwierzytelniania wzajemnego TLS (Mutual TLS). Protokół na poziomie aplikacji jest zastrzeżonym rozwiązaniem firmy Acronis. Węzeł magazynowania komunikuje się z systemami pamięci masowej na zapleczu przy użyciu odpowiednich protokołów i mechanizmów uwierzytelniania.

Wykaz jest pomocniczym komponentem rozwiązania Acronis Cyber Protect. Usługa ta indeksuje dane na węźle magazynowania, uzyskując do nich dostęp na porcie 9876, a indeks udostępnia na porcie 9200.

Brama kopii zapasowych implementuje nową generację protokołu dostępu do danych będącego zastrzeżoną technologią firmy Acronis. Ten sam komponent jest używany w rozwiązaniu Acronis Cyber Cloud, jeśli klient zdecyduje się na kopie zapasowe w chmurze. Brama używa portu TCP 44445, zarejestrowanego w IANA. Ochrona danych odbywa się za pomocą protokołu TLS, a do uwierzytelniania jest używana technologia uwierzytelniania wzajemnego TLS (Mutual TLS). Brama kopii zapasowych może też używać portu 8888 na potrzeby usługi zarządzania opartej na protokole HTTPS.

Agent komunikuje się z serwerem zarządzania, węzłem magazynowania i bramą kopii zapasowych za pośrednictwem portów, jak opisano powyżej. Agent może też komunikować się z opartymi na standardach usługami plików (SMB, NFS), jeśli są one używane jako miejsce docelowe kopii zapasowych. W takim przypadku używane są standardowe porty i odpowiednie protokoły uwierzytelniania. Agent dla VMware korzysta z interfejsu VMware vSphere API za pośrednictwem portów zdefiniowanych przez środowisko VMware vSphere, jeśli taka funkcja została skonfigurowana.

Ocena luk w zabezpieczeniach dla systemu Linux jest implementowana przy użyciu usługi CVSS, wdrożonej w rozwiązaniu Acronis Cyber Cloud. Agenty ochrony mogą dynamicznie wybierać najbliższe centrum danych na podstawie wyników polecenia ping z listy https://cloud.acronis.com/services.json.

Wdrożenie lokalne

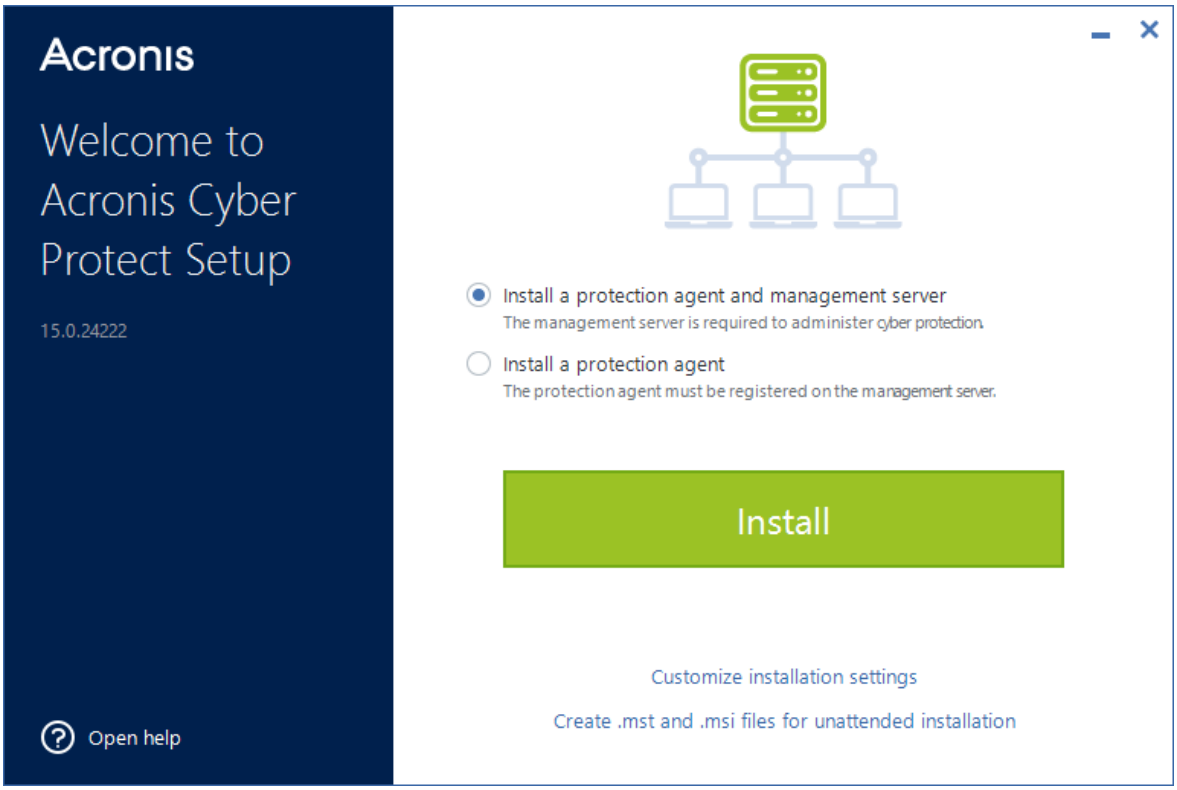
Wdrożenie lokalne obejmuje szereg komponentów oprogramowania, które opisano w sekcji "Komponenty" (s. 48). Szczegółowe informacje na temat interakcji między tymi komponentami a wymaganymi portami zawiera sekcja "Diagram połączenia sieciowego dla Acronis Cyber Protect" (s. 83).

Instalowanie serwera zarządzania

Instalacja w systemie Windows

Aby zainstalować serwer zarządzania

1. Zaloguj się jako administrator i uruchom program instalacyjny produktu Acronis Cyber Protect.
2. [Opcjonalnie] Aby zmienić język programu instalacyjnego, kliknij **Skonfiguruj język**.
3. Zaakceptuj warunki umowy licencyjnej i zasady ochrony prywatności, a następnie kliknij **Kontynuuj**.
4. Pozostaw ustawienie domyślne **Zainstaluj agenta ochrony i serwer zarządzania**.



5. Wykonaj dowolne z następujących czynności:

- Kliknij **Zainstaluj**.

  Jest to najprostszy sposób instalacji tego programu. Większość parametrów instalacji uzyska wartości domyślne.

  Zostaną zainstalowane następujące komponenty:

  - Serwer zarządzania
  - Komponenty do instalacji zdalnej
  - 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
  - Cyber Protect Monitor
- Kliknij **Dostosuj ustawienia instalacji**, aby skonfigurować instalację.

  Możesz wybrać komponenty do zainstalowania i określić dodatkowe parametry. Szczegółowe informacje można znaleźć w artykule "Dostosowywanie ustawień instalacji" (s. 88).
- Kliknij **Utwórz pliki .mst i .msi na potrzeby instalacji nienadzorowanej**, aby wyodrębnić pakiety instalacyjne. Przejrzyj lub zmodyfikuj ustawienia instalacji, które zostaną dodane do pliku .mst, a następnie kliknij **Generuj**. Kolejne kroki tej procedury nie są wymagane.

  Jeśli chcesz wdrożyć agenty przy użyciu zasad grupy, zapoznaj się z sekcją "Wdrażanie agentów przy użyciu zasad grupy" (s. 182).

6. Kontynuuj instalację.
7. Po zakończeniu instalacji kliknij **Zamknij**.

Aby rozpocząć korzystanie z serwera zarządzania, należy go aktywować, logując się na koncie Acronis lub przy użyciu pliku aktywacyjnego.

Dostosowywanie ustawień instalacji

W tej sekcji opisano ustawienia, które można zmienić podczas instalacji.

Komponenty do zainstalowania

W zależności od tego, czy jest instalowany serwer zarządzania i agent ochrony, czy tylko agent ochrony, domyślnie zostają wybrane następujące komponenty:

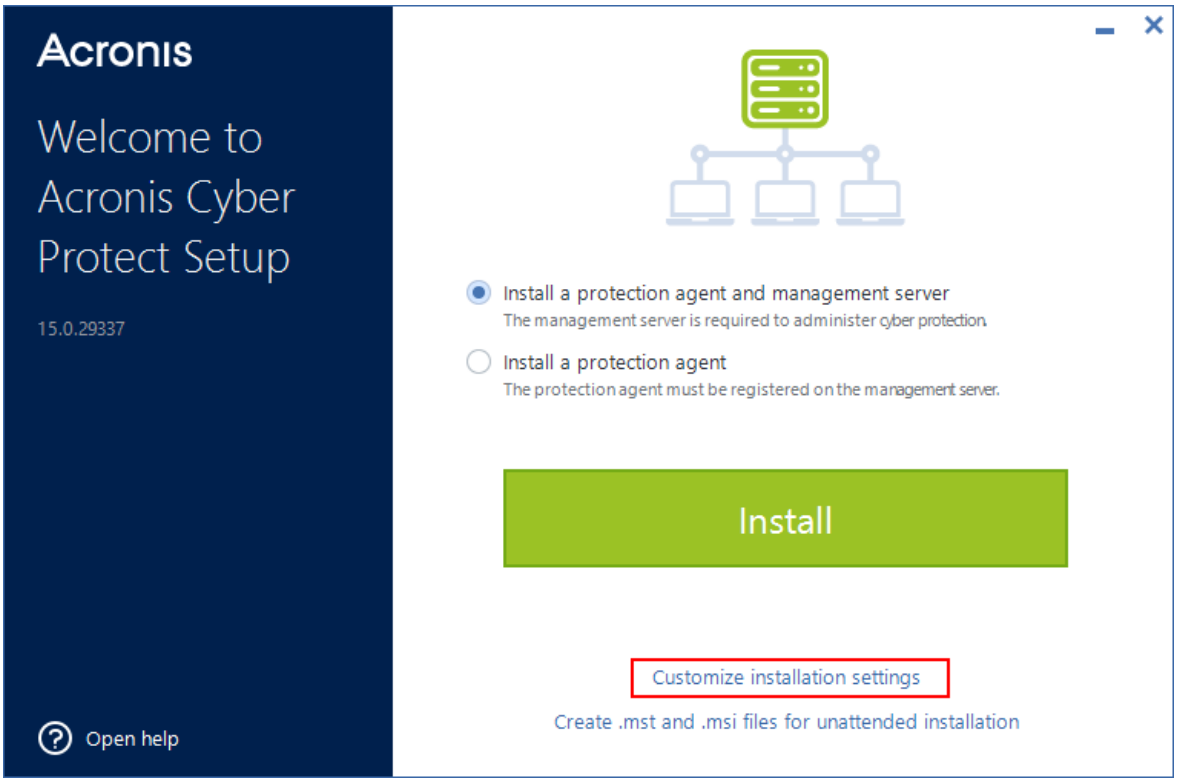
Serwer zarządzania i agent ochrony	Tylko agent ochrony
Serwer zarządzania	Agent dla systemu Windows
Komponenty do instalacji zdalnej	Generator nośnika startowego
Agent dla systemu Windows	Narzędzie wiersza polecenia

Serwer zarządzania i agent ochrony	Tylko agent ochrony
Generator nośnika startowego	Cyber Protect Monitor
Narzędzie wiersza polecenia	
Cyber Protect Monitor	

Pełną listę dostępnych komponentów można znaleźć w sekcji "Komponenty" (s. 48).

Aby zainstalować komponenty opcjonalne

1. W kreatorze instalacji kliknij **Dostosuj ustawienia instalacji**.



2. W obszarze **Elementy do zainstalowania** kliknij **Zmień**.
3. Wybierz właściwe komponenty i kliknij **Gotowe**.
4. Jeśli pojawi się monit o skonfigurowanie ustawień wybranych komponentów, zrób to.
5. Kliknij **Zainstaluj**.

Konto logowania usługi

Konto, na którym będzie działał agent lub usługa serwera zarządzania, można zmienić za pomocą odpowiedniej opcji: **Konto logowania dla usługi agenta** lub **Konto logowania dla usługi serwera zarządzania**.

Możesz wybrać jedną z poniższych opcji:

- **Użyj kont użytkowników usługi** (domyślne w przypadku usługi agenta)

  Konta użytkowników usługi to konta w systemie Windows używane do uruchamiania usług. Opcja ta ma tę zaletę, że zasady zabezpieczeń domeny nie wpływają na prawa użytkowników tych kont. Domyślnie agent działa na koncie **System lokalny**.
- **Utwórz nowe konto** (domyślne w przypadku usługi serwera zarządzania oraz usługi węzła magazynowania)

  Konta będą się nazywać **Acronis Agent User**, **AMS User** oraz **ASN User** w przypadku odpowiednio usług agenta, serwera zarządzania i węzła magazynowania.
- **Użyj następującego konta**

  Jeśli program zostanie zainstalowany na kontrolerze domeny, program instalacyjny wyświetli monit o określenie istniejących już kont (lub tego samego konta) na potrzeby poszczególnych usług. Ze względów bezpieczeństwa program instalacyjny nie tworzy automatycznie nowych kont na kontrolerze domeny.

  Konto użytkownika określone podczas uruchamiania programu instalacyjnego na kontrolerze domeny musi mieć przyznane prawo `Logowanie jako usługa`. Konto to musi już być używane na kontrolerze domeny, aby jego folder profilu został utworzony na tym komputerze.

  Dodatkowe informacje o instalowaniu agenta na kontrolerze domeny w trybie tylko do odczytu można znaleźć w tym artykule z bazy wiedzy Knowledge Base.

  Wybranie opcji **Użyj następującego konta** umożliwia także korzystanie z uwierzytelniania systemu Windows na potrzeby programu Microsoft SQL Server w przypadku skonfigurowania serwera zarządzania z bazą danych SQL.

W przypadku wybrania opcji **Utwórz nowe konto** lub **Użyj następującego konta** dopilnuj, aby zasady zabezpieczeń domeny nie wpływały na prawa powiązanych kont. Jeśli konto straci prawa użytkownika przypisane podczas instalacji, powiązany komponent może działać niepoprawnie lub wcale nie działać.

Wymagane prawa użytkownika w przypadku konta logowania usługi

Agent ochrony jest uruchamiany jako usługa **Managed Machine Service** (MMS) na komputerze z systemem Windows. Aby agent działał jak należy, konto, na którym jest uruchamiany, musi mieć następujące prawa:

1. Użytkownik usługi MMS musi należeć do grup **Operatorzy kopii zapasowych** i **Administratorzy**. W przypadku kontrolera domeny użytkownik musi należeć do grupy **Administratorzy domeny**.
2. Użytkownik usługi MMS musi mieć przyznane uprawnienie **Pełna kontrola** do folderu `%PROGRAMDATA%\Acronis` (w systemach Windows XP i Server 2003: `%ALLUSERSPROFILE%\Application Data\Acronis`) i jego podfolderów.
3. Użytkownik usługi MMS musi mieć przyznane uprawnienie **Pełna kontrola** do pewnych kluczy rejestru w kluczu: `HKEY_LOCAL_MACHINE\SOFTWARE\Acronis`.

4. Użytkownik usługi MMS musi mieć przyznane następujące prawa użytkownika w systemie Windows:
   - **Logowanie w trybie usługi**
   - **Dostosuj przydziały pamięci dla procesów**
   - **Zamień token na poziomie procesu**
   - **Modyfikuj wartości środowiskowe oprogramowania układowego**

Użytkownik ASN musi mieć prawa lokalnego administratora na komputerze z zainstalowanym programem Acronis Storage Node.

Aby przypisać prawa użytkownika w systemie Windows

Uwaga
W tej procedurze posłużono się przykładem prawa użytkownika **Logowanie w trybie usługi**. W przypadku innych praw użytkownika należy postępować tak samo.

1. Zaloguj się na komputerze jako administrator.
2. W obszarze **Panel sterowania** otwórz **Narzędzia administracyjne**. Możesz też nacisnąć klawisze Win+R i wpisać „**control admintools**”, a następnie nacisnąć klawisz Enter.
3. Otwórz **Zasady zabezpieczeń lokalnych**.
4. Rozwiń węzeł **Zasady lokalne** i kliknij **Przypisywanie praw użytkownika**.
5. W prawym okienku kliknij prawym przyciskiem myszy **Logowanie w trybie usługi** i wybierz **Właściwości**.
6. Kliknij **Dodaj użytkownika lub grupę**, aby dodać nowego użytkownika.
7. W oknie **Wybierz użytkowników lub grupy** znajdź użytkownika, którego chcesz dodać, i kliknij **OK**.
8. W oknie **Logowanie w trybie usługi > Właściwości** kliknij **OK**, aby zapisać zmiany.

Uwaga
Użytkownik dodany do prawa **Logowanie w trybie usługi** nie może się znajdować się na liście zasad **Odmowa logowania w trybie usługi** w obszarze **Zasady zabezpieczeń lokalnych**.

Ważne
Nie zaleca się ręcznej zmiany konta logowania po zakończeniu instalacji.

Baza danych na potrzeby serwera zarządzania

Można skonfigurować serwer zarządzania z następującymi bazami danych:

- SQLite

  Domyślnie serwer zarządzania korzysta z wbudowanej bazy danych SQLite. Umożliwia to zarejestrowanie na serwerze zarządzania około 900–1000 obciążeń. Baza danych SQLite nie jest zgodna z usługą Skanowanie.

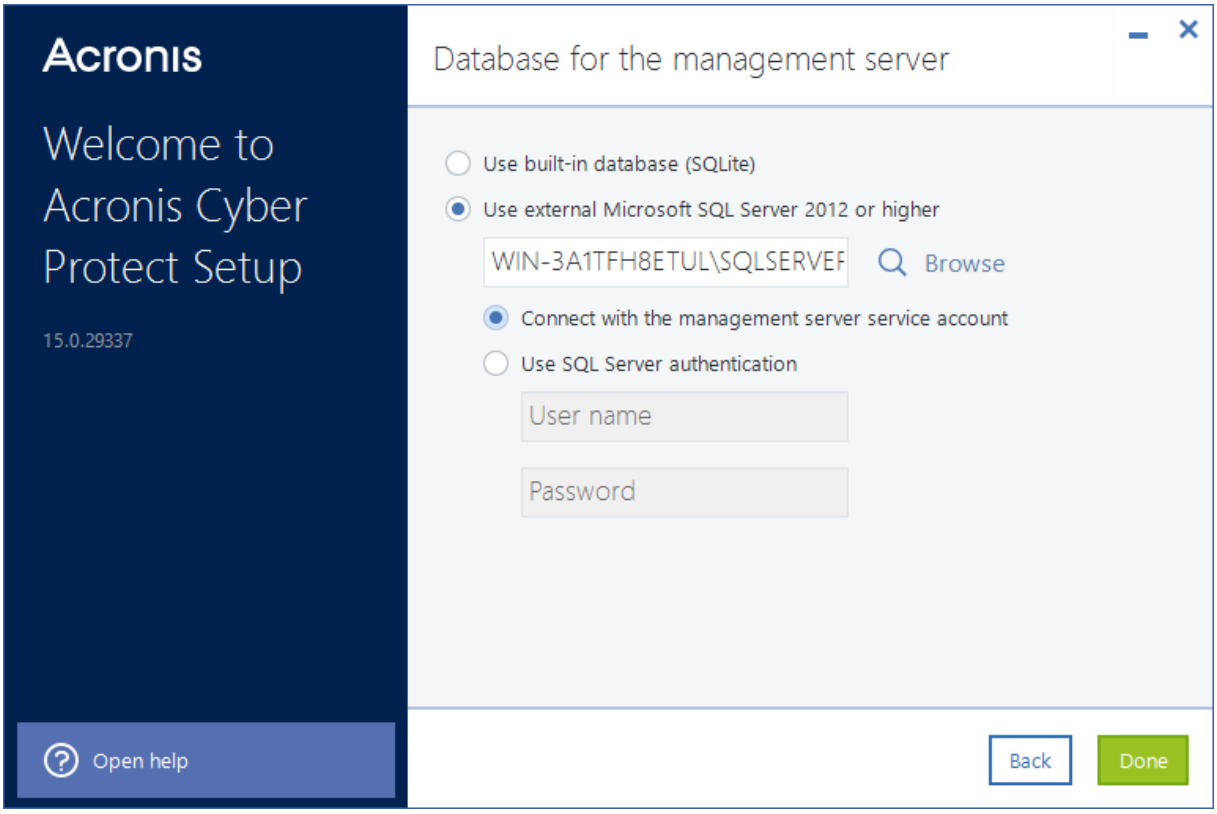
- Microsoft SQL

  Baza danych Microsoft SQL umożliwia zarejestrowanie na serwerze zarządzania nawet 8000 obciążeń bez zauważalnego spadku wydajności. Z jednej instancji bazy danych Microsoft SQL może korzystać serwer zarządzania, usługa Skanowanie i inne programy.

  Obsługiwane są następujące wersje programu MS SQL Server:

  - Microsoft SQL Server 2019 (działający w systemie Windows)
  - Microsoft SQL Server 2017 (działający w systemie Windows)
  - Microsoft SQL Server 2016
  - Microsoft SQL Server 2014
  - Microsoft SQL Server 2012

Jeśli instancja bazy danych Microsoft SQL ma nazwę domyślną **MSSQLSERVER**, wystarczy podać tylko nazwę komputera, na którym ta instancja działa. Jeśli instancja ma niestandardową nazwę, trzeba ją podać w następującym formacie: `nazwa komputera\nazwa instancji`.



Uwaga

Upewnij się, że na komputerze, na którym działa instancja bazy danych Microsoft SQL, włączono usługę Przeglądarka SQL Server oraz protokół TCP/IP. Dodatkowe informacje na temat uruchamiania usługi Przeglądarka SQL Server można znaleźć w artykule http://msdn.microsoft.com/en-us/library/ms189093.aspx. Protokół TCP/IP można włączyć, wykonując podobną procedurę.

Aby nawiązać połączenie z określoną instancją bazy danych Microsoft SQL, można skorzystać z następujących metod uwierzytelniania:

- Uwierzytelnianie systemu Windows (**Połącz z kontem usługi serwera zarządzania**)
  Z tej metody można skorzystać, jeśli konto logowania do usługi serwera zarządzania zostało skonfigurowane przy użyciu opcji **Użyj następującego konta**, na przykład przez wpisanie wartości `<NAZWA KOMPUTERA>\Administrator`. Wskazane konto musi mieć rolę **dbcreator** lub **sysadmin** w bazie danych Microsoft SQL Server.
  Dodatkowe informacje o koncie logowania można znaleźć w sekcji "Wymagane prawa użytkownika w przypadku konta logowania usługi" (s. 90).
- Uwierzytelnianie serwera SQL
  Z tej metody zawsze można skorzystać. Wskazane konto musi mieć rolę **dbcreator** lub **sysadmin** w bazie danych Microsoft SQL Server.

Usługa Skanowanie

Usługa Skanowanie to komponent opcjonalny, który umożliwia skanowanie antywirusowe kopii zapasowych w chmurze, w folderze lokalnym lub w folderze sieciowym. Usługa Skanowanie wymaga, aby na tym samym komputerze był zainstalowany serwer zarządzania.

Zainstalowanie usługi Skanowanie zapewnia dostęp do następujących funkcji:

- Plany skanowania kopii zapasowych
- Widżet Szczegóły skanowania kopii zapasowej
- Firmowa biała lista
- Bezpieczne odzyskiwanie
- Kolumna **Status** na liście kopii zapasowych

Usługę Skanowanie można zainstalować podczas instalacji serwera zarządzania lub dodać później, modyfikując instalację. Dodatkowe informacje na temat instalowania komponentów opcjonalnych, takich jak usługa Skanowanie, można znaleźć w sekcji "Aby zainstalować komponenty opcjonalne" (s. 89).

Ważne
Usługa Skanowanie nie jest zgodna z domyślną bazą danych SQLite używaną przez serwer zarządzania.

Usługę Skanowanie można skonfigurować z bazą danych Microsoft SQL lub PostgreSQL. Dodatkowe informacje na temat wybierania bazy danych można znaleźć w sekcji "Baza danych na potrzeby usługi Skanowanie" (s. 94).

Baza danych na potrzeby usługi Skanowanie

Usługa Skanowanie nie jest zgodna z bazą danych SQLite, czyli domyślną bazą danych serwera zarządzania.

Jeśli serwer zarządzania korzysta z bazy danych SQLite, usługę Skanowanie można skonfigurować tylko z bazą danych PostgreSQL. Obsługiwane jest oprogramowanie PostgreSQL w wersji 9.6 lub nowszej.

Jeśli serwer zarządzania korzysta z bazy danych Microsoft SQL Server, usługę Skanowanie można skonfigurować z tą samą bazą danych bez wprowadzania dodatkowych ustawień. Usługę Skanowanie można też skonfigurować z bazą danych PostgreSQL.

Aby skonfigurować usługę Skanowanie z bazą danych PostgreSQL

1. W kreatorze instalacji, w obszarze **Baza danych na potrzeby usługi Skanowanie** kliknij **Zmień**.
2. Zaznacz **Baza danych serwera PostgreSQL**.
3. Podaj nazwę hosta lub adres IP i port instancji bazy danych PostgreSQL.
4. Podaj poświadczenia użytkownika, który ma uprawnienie **CREATEDB** lub jest superużytkownikiem.

   Uwaga
   Metoda uwierzytelniania SCRAM-SHA-256 nie jest obsługiwana w oprogramowaniu PostgreSQL w wersji 10 lub nowszej.

5. Kliknij **Gotowe**.

Porty

Możesz skonfigurować port, którego przeglądarka internetowa będzie używać w celu uzyskania dostępu do serwera zarządzania (domyślnie jest to port 9877), i port, który będzie używany do komunikacji między komponentami produktu (domyślnie jest to port 7780). Zmiana tego drugiego portu po zakończeniu instalacji będzie wymagać ponownego zarejestrowania wszystkich komponentów.

Zapora systemu Windows jest automatycznie konfigurowana podczas instalacji. W przypadku korzystania z innej zapory należy się upewnić, że porty są otwarte zarówno dla żądań przychodzących, jak i wychodzących przez tę zaporę.

Serwer proxy

Można określić, czy podczas tworzenia kopii zapasowych do chmury oraz odzyskiwania z niej agenty ochrony mają używać serwera proxy HTTP.

Ponadto ten sam serwer proxy jest używany do komunikacji między różnymi komponentami programu Acronis Cyber Protect.

Aby był używany serwer proxy, podaj jego nazwę hosta lub adres IP i numer portu. Jeśli serwer proxy wymaga uwierzytelniania, podaj poświadczenia dostępu.

Uwaga
W przypadku korzystania z serwera proxy aktualizacja definicji ochrony (definicji ochrony przed wirusami i złośliwym oprogramowaniem, definicji zaawansowanego wykrywania, definicji oceny luk w zabezpieczeniach i zarządzania poprawkami) nie jest możliwa.

Instalacja w systemie Linux

Przygotowanie

1. Aby razem z serwerem zarządzania zainstalować agenta dla systemu Linux, upewnij się, że na komputerze są zainstalowane niezbędne pakiety systemu Linux.
2. Wybierz bazę danych, która będzie używana przez serwer zarządzania.

Ograniczenie

Serwery zarządzania na komputerach z systemem Linux nie obsługują zdalnej instalacji agentów ochrony, która jest stosowana na przykład w przypadku procedury wykrywania automatycznego. Więcej informacji na temat możliwych obejść można znaleźć w bazie wiedzy Knowledge Base: https://kb.acronis.com/content/69553.

Instalacja

Aby zainstalować serwer zarządzania, potrzebujesz co najmniej 4 GB wolnego miejsca na dysku.

Aby zainstalować serwer zarządzania

1. Jako użytkownik root przejdź do katalogu z plikiem instalacyjnym, zmień plik w plik wykonywalny, a następnie go uruchom.

   ```
   chmod +x <installation file name>
   ```

   ```
   ./<installation file name>
   ```

2. Zaakceptuj warunki umowy licencyjnej.
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 internetowa Cyber Protect.

Aby rozpocząć korzystanie z serwera zarządzania, należy go aktywować, logując się na koncie Acronis lub przy użyciu pliku aktywacyjnego.

Urządzenie Acronis Cyber Protect

Wraz z urządzeniem Acronis Cyber Protect można łatwo uzyskać maszynę wirtualną z następującym oprogramowaniem:

- CentOS
- Komponenty programu Acronis Cyber Protect
  - Serwer zarządzania
  - Agent dla systemu Linux
  - Agent dla VMware (Linux)

Urządzenie jest udostępniane jako archiwum .zip. Archiwum to zawiera pliki .ovf oraz .iso. Można wdrożyć plik .ovf na hoście ESXi lub użyć pliku .iso do uruchomienia istniejącej już maszyny wirtualnej. Archiwum zawiera też plik .vmdk, który należy umieścić w tym samym katalogu co plik .ovf.

Uwaga
VMware Host Client (klient internetowy używany do zarządzania autonomicznym hostem ESXi 6.0+) nie umożliwia wdrażania szablonów OVF zawierających obraz ISO. Jeśli korzystasz z tego rozwiązania, utwórz maszynę wirtualną, która spełnia poniższe wymagania, i zainstaluj oprogramowanie przy użyciu pliku .iso.

Wymagania dotyczące urządzenia wirtualnego:

- Minimalne wymagania systemowe:
  - 2 procesory
  - 6 GB pamięci RAM
  - Jeden dysk wirtualny o pojemności 10 GB (zaleca się pojemność 40 GB)
- W ustawieniach maszyny wirtualnej VMware kliknij kartę **Opcje** > **Ogólne** > **Parametry konfiguracji** i upewnij się, że parametr `disk.EnableUUID` ma wartość `true`.

Ograniczenie

Serwery zarządzania na komputerach z systemem Linux, w tym urządzenie Acronis Cyber Protect, nie obsługują zdalnej instalacji agentów ochrony, która jest stosowana na przykład w przypadku

procedury wykrywania automatycznego. Więcej informacji na temat możliwych obejść można znaleźć w bazie wiedzy Knowledge Base: https://kb.acronis.com/content/69553.

Instalowanie oprogramowania

1. Wykonaj jedną z następujących czynności:
   - Wdróż urządzenie z pliku .ovf. Zakończywszy wdrożenie, włącz powstałą maszynę wirtualną.
   - Uruchom istniejącą już maszynę wirtualną z obrazu .iso.
2. Wybierz **Zainstaluj lub zaktualizuj program Acronis Cyber Protect**, a następnie naciśnij klawisz **Enter**. Poczekaj, aż pojawi się początkowe okno instalacji.
3. [Opcjonalnie] Aby zmienić ustawienia instalacji, wybierz **Zmień ustawienia**, a następnie naciśnij **Enter**. Można określić następujące ustawienia:
   - Nazwa hosta urządzenia (domyślnie: `AcronisAppliance-<część losowa>`).
   - Hasło do konta „root”, które będzie używane do logowania się do konsoli internetowej Cyber Protect (domyślnie **nie jest określone**).

     Jeśli zostawisz wartość domyślną, po zakończeniu instalacji programu Acronis Cyber Protect pojawi się monit o określenie hasła. Bez tego hasła nie będzie można się zalogować do konsoli internetowej Cyber Protect ani do konsoli internetowej Cockpit.
   - Ustawienia sieci karty sieciowej:
     - **Używaj usługi DHCP** (domyślne)
     - **Ustaw statyczny adres IP**

     Jeśli komputer ma kilka kart sieciowych, oprogramowanie losowo wybierze jedną z nich i zastosuje do niej te ustawienia.
4. Wybierz **Zainstaluj przy użyciu bieżących ustawień**.

W wyniku tego na komputerze zostanie zainstalowany system CentOS i program Acronis Cyber Protect.

Kolejne działania

Po zakończeniu instalacji oprogramowanie wyświetli łącza do konsoli internetowej Cyber Protect i konsoli internetowej Cockpit. Ustanów połączenie z konsolą internetową Cyber Protect, aby zacząć korzystać z programu Acronis Cyber Protect: dodać kolejne urządzenia, utworzyć plany tworzenia kopii zapasowych itd.

Aby dodać maszyny wirtualne ESXi, kliknij **Dodaj** > **VMware ESXi**, a następnie określ adres i poświadczenia serwera vCenter lub autonomicznego hosta ESXi.

W konsoli internetowej Cockpit nie konfiguruje się żadnych ustawień programu Acronis Cyber Protect. Konsola ta jest udostępniana dla wygody i na potrzeby rozwiązywania problemów.

Aktualizowanie oprogramowania

1. Pobierz i rozpakuj archiwum .zip z nową wersją urządzenia.
2. Uruchom komputer z obrazu .iso wypakowanego w poprzednim kroku.
   a. Zapisz obraz .iso w magazynie danych vSphere.
   b. Podłącz obraz .iso do napędu CD/DVD komputera.
   c. Uruchom ponownie komputer.
   d. [Tylko podczas pierwszej aktualizacji] Naciśnij klawisz **F2**, a następnie zmień kolejność startową w taki sposób, aby napęd CD/DVD był pierwszy.
3. Wybierz **Zainstaluj lub zaktualizuj program Acronis Cyber Protect**, a następnie naciśnij klawisz **Enter**.
4. Wybierz **Aktualizuj**, a następnie naciśnij **Enter**.
5. Po zakończeniu aktualizacji odłącz obraz .iso od napędu CD/DVD komputera.

W wyniku tego zostanie zaktualizowany program Acronis Cyber Protect. Jeśli wersja systemu CentOS w pliku .iso jest nowsza od wersji na dysku, przed zaktualizowaniem programu Acronis Cyber Protect zostanie zaktualizowany system operacyjny.

Dodawanie komputerów w konsoli internetowej Cyber Protect

Możesz dodać komputer na jeden z następujących sposobów:

- Pobranie programu instalacyjnego i jego lokalne uruchomienie na komputerze docelowym.
- Zdalne zainstalowanie agenta ochrony na komputerze docelowym.

Ograniczenia

- Instalacja zdalna jest dostępna tylko w przypadku serwera zarządzania działającego na komputerze z systemem Windows. Na komputerach docelowych również musi działać system Windows.
- Instalacja zdalna nie jest obsługiwana na komputerach z systemem Windows XP.
- Instalacja zdalna nie jest obsługiwana na kontrolerach domen. Instrukcje instalacji agenta ochrony na kontrolerze domeny można znaleźć w sekcji "Instalacja w systemie Windows" (s. 107). Zadbaj, aby ustawienia instalacji były odpowiednio dostosowane, wybierając **Użyj następującego konta** w obszarze **Konto logowania dla usługi agenta**. Dodatkowe informacje na temat tej opcji można znaleźć w sekcji "Wymagane prawa użytkownika w przypadku konta logowania usługi" (s. 90).

Dodawanie komputera z systemem Windows

Komputer z systemem Windows można dodać przez zdalne zainstalowanie agenta ochrony w konsoli internetowej Cyber Protect lub pobranie programu instalacyjnego i jego lokalne

uruchomienie.

Aby zainstalować agenta zdalnie

Ważne
Przed rozpoczęciem instalacji należy dopilnować, aby zostały spełnione warunki instalacji zdalnej, a w środowisku był co najmniej jeden agent, którego można użyć jako agenta wdrażania. Dodatkowe informacje można znaleźć w sekcjach "Wymagania wstępne dotyczące instalacji zdalnej" (s. 100) i "Agent wdrażania" (s. 102).

1. W konsoli internetowej Cyber Protect przejdź do sekcji **Urządzenia** > **Wszystkie urządzenia**.
2. Kliknij **Dodaj**.
3. [W celu zainstalowania agenta dla systemu Windows] Kliknij **Windows**.
4. [W celu zainstalowania innego obsługiwanego agenta] Kliknij przycisk odpowiadający aplikacji, którą chcesz chronić.
   Dostępne są następujące agenty:
   - Agent dla Hyper-V
   - Agent dla SQL + agent dla systemu Windows
   - Agent dla programu Exchange + agent dla systemu Windows
     W przypadku kliknięcia **Microsoft Exchange Server** > **Skrzynki pocztowe programu Exchange** i zarejestrowania co najmniej jednego agenta dla programu Exchange przejdź do kroku 9.
   - Agent dla usługi Active Directory + agent dla systemu Windows
   - Agent dla usługi Office 365
5. W otwartym panelu wybierz agenta wdrażania.
6. Określ nazwę hosta lub adres IP komputera docelowego oraz poświadczenia dostępu do znajdującego się na tym komputerze konta z prawami administracyjnymi.
   Zalecamy skorzystanie z wbudowanego konta administratora. Aby użyć innego konta, należy je dodać do grupy Administratorzy i zmodyfikować rejestr na komputerze docelowym zgodnie z opisem podanym w następującym artykule: https://support.microsoft.com/en-us/help/951016/description-of-user-account-control-and-remote-restrictions-in-windows.
7. Wybierz nazwę lub adres IP serwera zarządzania, których agent będzie używać w celu uzyskania dostępu do tego serwera.
   Domyślnie wybrana jest nazwa serwera. Jeśli serwer zarządzania ma więcej niż jeden interfejs sieciowy lub występują problemy z usługą DNS, które powodują niepowodzenie rejestracji agenta, może być konieczne wybranie adresu IP.
8. Kliknij **Zainstaluj**.
9. [Jeśli w kroku 4 wybrano **Microsoft Exchange Server** > **Skrzynki pocztowe programu Exchange**] Wskaż komputer z włączoną rolą serwera **Dostęp klienta** programu Microsoft

Exchange Server. Więcej informacji można znaleźć w sekcji "Kopia zapasowa skrzynki pocztowej" (s. 468).

Aby pobrać agenta i zainstalować go lokalnie

1. W konsoli internetowej Cyber Protect kliknij ikonę konta widoczną w prawym górnym rogu, a następnie kliknij **Do pobrania**.
2. Kliknij nazwę potrzebnego instalatora systemu Windows.
   Program instalacyjny zostanie pobrany na Twój komputer.
3. Na komputerze, który chcesz objąć ochroną, uruchom program instalacyjny. Więcej informacji można znaleźć w sekcji "Instalacja w systemie Windows" (s. 107).

Wymagania wstępne dotyczące instalacji zdalnej

- Aby można było pomyślnie przeprowadzić instalację na komputerze zdalnym z systemem Windows 7 lub nowszym, musi na nim być wyłączona opcja **Panel sterowania** > **Opcje folderów** > **Widok** > **Użyj Kreatora udostępniania**.
- Aby pomyślnie przeprowadzić instalację na komputerze zdalnym, który *nie* należy do domeny Active Directory, musi na nim być *wyłączona* funkcja Kontrola konta użytkownika (UAC). Dodatkowe informacje o tym, jak ją wyłączyć, można znaleźć w sekcji "Aby wyłączyć funkcję UAC" (s. 101).
- Domyślnie do instalacji na dowolnym komputerze zdalnym z systemem Windows są wymagane poświadczenia dostępu do wbudowanego konta użytkownika Administrator. Aby przeprowadzić instalację zdalną przy użyciu poświadczeń dostępu do innego konta administratora, należy *wyłączyć* ograniczenia funkcji UAC dotyczące połączeń zdalnych. Dodatkowe informacje o tym, jak je wyłączyć, można znaleźć w sekcji "Aby wyłączyć ograniczenia funkcji UAC dotyczące połączeń zdalnych" (s. 101).
- Na komputerze zdalnym należy *włączyć* udostępnianie plików i drukarek. Aby uzyskać dostęp do tej opcji:
  - [Na komputerze z systemem Windows Server 2003] Wybierz **Panel sterowania** > **Zapora systemu Windows** > **Wyjątki** > **Udostępnianie plików i drukarek**.
  - [Na komputerze z systemem Windows Server 2008, Windows 7 lub nowszym] Wybierz **Panel sterowania** > **Zapora systemu Windows** > **Centrum sieci i udostępniania** > **Zmień zaawansowane ustawienia udostępniania**.
- Program Acronis Cyber Protect używa do instalacji zdalnej portów TCP **445**, **25001** i **43234**.
  Port **445** jest automatycznie otwierany po wybraniu opcji Udostępnianie plików i drukarek. Porty 43234 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 port **25001** jest automatycznie zamykany przez Zaporę systemu Windows. Jeśli chcesz aktualizować agenta zdalnie w przyszłości, porty **445** i **43234** muszą pozostać otwarte. Przy każdej aktualizacji port **25001** jest automatycznie ponownie otwierany i zamykany przez Zaporę systemu Windows. W przypadku korzystania z innej zapory sieciowej wszystkie trzy porty pozostaną otwarte.

Uwaga
Instalacja zdalna nie jest obsługiwana na komputerach z systemem Windows XP.

Uwaga
Instalacja zdalna nie jest obsługiwana na kontrolerach domen. Instrukcje instalacji agenta ochrony na kontrolerze domeny można znaleźć w sekcji "Instalacja w systemie Windows" (s. 107). Zadbaj, aby ustawienia instalacji były odpowiednio dostosowane, wybierając **Użyj następującego konta** w obszarze **Konto logowania dla usługi agenta**. Dodatkowe informacje na temat tej opcji można znaleźć w sekcji "Wymagane prawa użytkownika w przypadku konta logowania usługi" (s. 90).

Wymagania dotyczące funkcji Kontrola konta użytkownika (UAC)

Na komputerze z systemem operacyjnym Windows 7 lub nowszym, który nie należy do domeny Active Directory, trzeba wyłączyć funkcję Kontrola konta użytkownika (UAC) i jej ograniczenia dotyczące połączeń zdalnych, 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 sekcji **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.

Aby wyłączyć ograniczenia funkcji UAC dotyczące połączeń zdalnych

1. Uruchom Edytor rejestru.
2. Odszukaj następujący klucz rejestru: **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System**
3. Zmień wartość **LocalAccountTokenFilterPolicy** na **1**.
   Jeśli wartość **LocalAccountTokenFilterPolicy** nie istnieje, utwórz ją jako DWORD (32-bitowy). Dodatkowe informacje na temat tej wartości można znaleźć w dokumentacji firmy Microsoft: https://support.microsoft.com/en-us/help/951016/description-of-user-account-control-and-remote-restrictions-in-windows.

Uwaga
Ze względów bezpieczeństwa zaleca się przywrócenie — po zakończeniu operacji zarządzania, np. instalacji zdalnej — obu ustawień do stanu pierwotnego: **EnableLUA**=**1** i **LocalAccountTokenFilterPolicy**=**0**.

Agent wdrażania

Aby zainstalować agenty ochrony na komputerach zdalnych z poziomu konsoli internetowej Cyber Protect, w środowisku musi już być zainstalowany co najmniej jeden agent. Agent ten będzie służyć jako agent wdrażania na potrzeby instalacji zdalnej i będzie się łączył z serwerem zarządzania oraz docelowym komputerem zdalnym.

Pierwszym agentem ochrony w środowisku jest zwykle agent zainstalowany wraz z serwerem zarządzania. Niemniej jednak każdego agenta dla systemu Windows w środowisku można wybrać jako agenta wdrażania.

Uwaga
W przypadku użycia funkcji wykrywania automatycznego w celu zainstalowania agentów ochrony na wielu komputerach agent wdrażania jest nazywany agentem wykrywania.

Zasady działania agenta wdrażania

1. Agent wdrażania łączy się z serwerem zarządzania i pobiera plik `web_installer.exe`.
2. Agent wdrażania łączy się z komputerem zdalnym przy użyciu nazwy hosta lub adresu IP tego komputera oraz podanych poświadczeń administratora, a następnie przesyła do niego plik `web_installer.exe`.
3. Plik `web_installer.exe` zostaje uruchomiony na komputerze zdalnym w trybie nienadzorowanym.
4. W zależności od zakresu wymaganej instalacji instalator internetowy pobiera dodatkowe pakiety instalacyjne z folderu `installation_files` na serwerze zarządzania, a następnie instaluje je na komputerze docelowym za pomocą polecenia `msiexec`.

   Folder `installation_files` znajduje się w następującym miejscu:
   - W systemie Windows: `\Program Files\Acronis\RemoteInstallationFiles\`
   - W systemie Linux: `/usr/lib/Acronis/RemoteInstallationFiles/`
5. Po zakończeniu instalacji agent zostaje zarejestrowany na serwerze zarządzania.

Komponenty do instalacji zdalnej

Komponenty do instalacji zdalnej są instalowane domyślnie podczas instalacji serwera zarządzania.

W zależności od systemu operacyjnego komputera, na którym działa serwer zarządzania, komponenty te można znaleźć w następujących lokalizacjach:

- Windows: `%Program Files%\Acronis\RemoteInstallationFiles\installation_files`
- Linux: `/usr/lib/Acronis/RemoteInstallationFiles/installation_files`

Lokalizacje te mogą być niedostępne w przypadku aktualizacji ze starszej wersji programu Acronis Cyber Protect lub wyraźnego wykluczenia pozycji **Komponenty do instalacji zdalnej** podczas instalowania serwera zarządzania. W takim przypadku należy ręcznie dodać komponenty do instalacji zdalnej, aktualizując i modyfikując istniejącą instalację programu Acronis Cyber Protect.

Aby dodać komponenty do instalacji zdalnej do istniejącej instalacji

1. Pobierz najnowszą wersję pliku instalacyjnego programu Acronis Cyber Protect z witryny internetowej firmy Acronis.
   Wybierz plik instalacyjny odpowiedni do bitowości systemu operacyjnego. W większości przypadków potrzebny będzie plik instalacyjny w wersji **Windows 64-bit**. W razie konieczności zdalnego zainstalowania agentów ochrony na komputerach z systemem 32-bitowym pobierz plik instalacyjny w wersji **Windows 32/64-bit**.
2. Na komputerze, na którym działa serwer zarządzania, uruchom plik instalacyjny, a następnie wybierz **Aktualizuj**.
3. Po zakończeniu aktualizacji ponownie uruchom plik instalacyjny, a następnie wybierz **Modyfikuj bieżącą instalację**.
4. Wybierz **Komponenty do instalacji zdalnej**, a następnie kliknij **Gotowe**.

Po zakończeniu instalacji będzie można zainstalować agenty ochrony na komputerach zdalnych z poziomu konsoli internetowej Cyber Protect.

Dodawanie komputera z systemem Linux

Komputer z systemem Linux można dodać tylko przez lokalne zainstalowanie agenta ochrony. Instalacja zdalna nie jest obsługiwana.

Aby dodać komputer z systemem Linux

1. W konsoli internetowej Cyber Protect kliknij **Wszystkie urządzenia** > **Dodaj**.
2. Kliknij **Linux**.
   Program instalacyjny zostanie pobrany na Twój komputer.
3. Na komputerze, który chcesz objąć ochroną, uruchom program instalacyjny. Więcej informacji można znaleźć w sekcji "Instalacja w systemie Linux" (s. 110).

Dodawanie komputera z systemem macOS

Komputer z systemem macOS można dodać tylko przez lokalne zainstalowanie agenta ochrony. Instalacja zdalna nie jest obsługiwana.

Aby dodać komputer z systemem macOS

1. W konsoli internetowej Cyber Protect kliknij **Wszystkie urządzenia** > **Dodaj**.
2. Kliknij **Mac**.

Program instalacyjny zostanie pobrany na Twój komputer.

3. Na komputerze, który chcesz objąć ochroną, uruchom program instalacyjny. Więcej informacji można znaleźć w sekcji "Instalacja w systemie macOS" (s. 111).

Dodawanie serwera vCenter lub hosta ESXi

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

- Wdrażanie agenta dla VMware (urządzenie wirtualne)

  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)

  Na potrzeby odciążonego tworzenia kopii zapasowych (tj. bez obciążania sieci lokalnej) można zainstalować agenta dla VMware na komputerze fizycznym z systemem Windows.
  - **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 „Tworzenie kopii zapasowych bez obciążania sieci lokalnej”.

  Jeśli serwer zarządzania działa w systemie Windows, agent zostanie automatycznie wdrożony na wskazanym komputerze. W przeciwnym razie agenta trzeba zainstalować ręcznie.
- Rejestrowanie już zainstalowanego agenta dla VMware

  Krok ten jest konieczny po ponownym zainstalowaniu serwera zarządzania. Ponadto można zarejestrować i skonfigurować agenta dla VMware (urządzenie wirtualne) wdrożonego przy użyciu szablonu OVF.
- Konfigurowanie już zarejestrowanego agenta dla VMware

  Krok ten jest konieczny po ręcznym zainstalowaniu agenta dla VMware (Windows) lub wdrożeniu urządzenia Acronis Cyber Protect. Ponadto można powiązać już skonfigurowanego agenta dla VMware z innym serwerem vCenter lub autonomicznym hostem ESXi.

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. Podaj adres serwera vCenter lub autonomicznego hosta ESXi i poświadczenia dostępu do niego. Zalecamy korzystanie z konta, które ma przypisaną rolę **Administrator**. W innym przypadku należy zadbać o dostęp do konta mającego niezbędne uprawnienia na serwerze vCenter lub ESXi.
5. Wybierz nazwę lub adres IP serwera zarządzania, których agent będzie używać w celu uzyskania dostępu do tego serwera.

   Domyślnie wybrana jest nazwa serwera. Jeśli serwer zarządzania ma więcej niż jeden interfejs sieciowy lub występują problemy z usługą DNS, które powodują niepowodzenie rejestracji agenta, może być konieczne wybranie adresu IP.
6. [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.
   - Ustawienia sieciowe urządzenia wirtualnego. Możesz wybrać automatyczną konfigurację DHCP lub ręcznie określić poszczególne wartości, w tym statyczny adres IP.
7. Kliknij **Wdróż**.

Instalowanie agenta dla VMware (Windows)

Przygotowanie

Wykonaj czynności przygotowawcze opisane w sekcji „Dodawanie komputera z systemem Windows”.

Instalacja

1. Kliknij **Wszystkie urządzenia** > **Dodaj**.
2. Kliknij **VMware ESXi**.
3. Wybierz **Zainstaluj zdalnie na komputerze z systemem Windows**.
4. Wybierz agenta wdrażania.
5. Określ nazwę hosta lub adres IP komputera docelowego oraz poświadczenia dostępu do znajdującego się na tym komputerze konta z uprawnieniami administracyjnymi.
6. Wybierz nazwę lub adres IP serwera zarządzania, których agent będzie używać w celu uzyskania dostępu do tego serwera.

   Domyślnie wybrana jest nazwa serwera. Jeśli serwer zarządzania ma więcej niż jeden interfejs sieciowy lub występują problemy z usługą DNS, które powodują niepowodzenie rejestracji agenta, może być konieczne wybranie adresu IP.

7. Kliknij **Połącz**.
8. 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 na serwerze vCenter lub ESXi.
9. 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".
- Agent dla VMware (Windows) jest rejestrowany podczas instalacji lokalnej.

Aby zarejestrować agenta dla VMware

1. Kliknij **Wszystkie urządzenia** > **Dodaj**.
2. Kliknij **VMware ESXi**.
3. Wybierz **Zarejestruj już zainstalowanego agenta**.
4. Wybierz agenta wdrażania.
5. Jeśli rejestrujesz *agenta dla VMware (Windows)*, określ nazwę hosta lub adres IP komputera, na którym ten agent jest zainstalowany, i poświadczenia dostępu do 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.
6. Wybierz nazwę lub adres IP serwera zarządzania, których agent będzie używać w celu uzyskania dostępu do tego serwera.

   Domyślnie wybrana jest nazwa serwera. Jeśli serwer zarządzania ma więcej niż jeden interfejs sieciowy lub występują problemy z usługą DNS, które powodują niepowodzenie rejestracji agenta, może być konieczne wybranie adresu IP.
7. Kliknij **Połącz**.
8. Podaj nazwę hosta lub adres IP serwera vCenter bądź 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 na serwerze vCenter lub ESXi.
9. Kliknij **Zarejestruj**, aby zarejestrować agenta.

Konfigurowanie już zarejestrowanego agenta dla VMware

W tej sekcji opisano, jak powiązać agenta dla VMware z serwerem vCenter lub hostem ESXi przy użyciu interfejsu internetowego. Można to też zrobić na konsoli agenta dla VMware (urządzenie wirtualne).

Za pomocą tej procedury można również zmienić istniejące już powiązanie agenta z serwerem vCenter lub hostem ESXi. Można to też zrobić na konsoli agenta dla VMware (urządzenie wirtualne), klikając **Ustawienia** > **Agenci** > agent > **Szczegóły** > **vCenter/ESXi**.

Aby skonfigurować agenta dla VMware

1. Kliknij **Wszystkie urządzenia** > **Dodaj**.
2. Kliknij **VMware ESXi**.
3. Oprogramowanie wyświetla nieskonfigurowanego agenta dla VMware, który pojawia się jako pierwszy na liście uporządkowanej w kolejności alfabetycznej.
   Jeśli wszystkie agenty zarejestrowane na serwerze zarządzania są już skonfigurowane, kliknij **Skonfiguruj już zarejestrowany agent**, a oprogramowanie wyświetli agenta, który jest pokazywany jako pierwszy na liście uporządkowanej w kolejności alfabetycznej.
4. W razie konieczności kliknij **Komputer z agentem** i wybierz agenta do skonfigurowania.
5. Określ albo zmień nazwę hosta lub adres IP serwera vCenter bądź hosta ESXi, a także poświadczenia umożliwiające uzyskanie do niego dostępu. Zalecamy korzystanie z konta, które ma przypisaną rolę **Administrator**. W innym przypadku należy zadbać o dostęp do konta mającego niezbędne uprawnienia na serwerze vCenter lub ESXi.
6. Kliknij **Skonfiguruj**, aby zapisać zmiany.

Dodawanie klastra Scale Computing HC3

Aby dodać klaster Scale Computing HC3 do serwera zarządzania Cyber Protect

1. Wdróż w klastrze agenta dla Scale Computing HC3 (urządzenie wirtualne).
2. Skonfiguruj jego połączenie zarówno z klastrem, jak i z serwerem zarządzania Cyber Protect.

Instalowanie agentów lokalnie

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 Cyber Protect.
2. [Opcjonalnie] Aby zmienić język programu instalacyjnego, kliknij **Skonfiguruj język**.
3. Zaakceptuj warunki umowy licencyjnej i zasady ochrony prywatności, a następnie kliknij **Kontynuuj**.

4. Wybierz **Zainstaluj agenta ochrony**.
5. Wykonaj dowolne z następujących czynności:
   - Kliknij **Zainstaluj**.

     Jest to najprostszy sposób instalacji tego programu. Większość parametrów instalacji uzyska wartości domyślne.

     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
     - Cyber Protect Monitor
   - Kliknij **Dostosuj ustawienia instalacji**, aby skonfigurować instalację.

     Możesz wybrać komponenty do zainstalowania i określić dodatkowe parametry. Szczegółowe informacje można znaleźć w artykule "Dostosowywanie ustawień instalacji" (s. 88).
   - Kliknij **Utwórz pliki .mst i .msi na potrzeby instalacji nienadzorowanej**, aby wyodrębnić pakiety instalacyjne. Przejrzyj lub zmodyfikuj ustawienia instalacji, które zostaną dodane do pliku .mst, a następnie kliknij **Generuj**. Kolejne kroki tej procedury nie są wymagane.

     Jeśli chcesz wdrożyć agenty przy użyciu zasad grupy, postępuj zgodnie z opisem podanym w sekcji "Wdrażanie agentów przy użyciu zasad grupy" (s. 182).
6. Określ serwer zarządzania, na którym zostanie zarejestrowany komputer z agentem:
   a. Określ nazwę hosta lub adresIP komputera, na którym jest zainstalowany serwer zarządzania.
   b. Podaj poświadczenia administratora serwera zarządzania lub token rejestracji.

      Dodatkowe informacje o procedurze generowania tokenu rejestracji można znaleźć w sekcji "Krok 1: Generowanie tokenu rejestracji" (s. 183).
   c. Kliknij **Gotowe**.
7. Jeśli pojawi się monit, wskaż, czy komputer z agentem zostanie dodany do organizacji, czy do jednej z jednostek.

   Monit pojawia się w sytuacji, gdy administrujesz więcej niż jedną jednostką lub organizacją mającą co najmniej jedną jednostkę. W przeciwnym razie komputer zostanie dodany w trybie dyskretnym do administrowanej jednostki lub organizacji. Więcej informacji można znaleźć w sekcji "Jednostki i konta administracyjne" (s. 666).
8. Kontynuuj instalację.
9. Po zakończeniu instalacji kliknij **Zamknij**.
10. Jeśli został zainstalowany agent dla programu Exchange, można tworzyć kopie zapasowych baz danych programu Exchange. Jeśli chcesz utworzyć kopię zapasową skrzynek pocztowych programu Exchange, otwórz konsolę internetową Cyber Protect, kliknij **Dodaj** > **Microsoft**

Exchange Server > **Skrzynki pocztowe programu Exchange**, a następnie wskaż komputer z włączoną rolą serwera **Dostęp klienta** programu Microsoft Exchange Server. Więcej informacji można znaleźć w sekcji "Kopia zapasowa skrzynki pocztowej" (s. 468).

Aby zainstalować agenta dla VMware (Windows), agenta dla usługi Office 365, agenta dla Oracle lub agenta dla programu Exchange na komputerze bez programu Microsoft Exchange Server

1. Zaloguj się jako administrator i uruchom program instalacyjny produktu Acronis Cyber Protect.
2. [Opcjonalnie] Aby zmienić język programu instalacyjnego, kliknij **Skonfiguruj język**.
3. Zaakceptuj warunki umowy licencyjnej i zasady ochrony prywatności, a następnie kliknij **Kontynuuj**.
4. Wybierz **Zainstaluj agenta ochrony**, a następnie kliknij **Dostosuj ustawienia instalacji**.
5. Obok pozycji **Elementy do zainstalowania** kliknij **Zmień**.
6. Zaznacz pole wyboru odpowiadające agentowi, którego chcesz zainstalować. Wyczyść pola wyboru odpowiadające komponentom, których nie chcesz instalować. Kliknij **Gotowe**, aby kontynuować.
7. Określ serwer zarządzania, na którym zostanie zarejestrowany komputer z agentem:
   a. Kliknij Określ obok pozycji **Acronis Cyber Protect Management Server**.
   b. Określ nazwę hosta lub adresIP komputera, na którym jest zainstalowany serwer zarządzania.
   c. Podaj poświadczenia administratora serwera zarządzania lub token rejestracji.
      Dodatkowe informacje o procedurze generowania tokenu rejestracji można znaleźć w sekcji "Krok 1: Generowanie tokenu rejestracji" (s. 183).
   d. Kliknij **Gotowe**.
8. Jeśli pojawi się monit, wskaż, czy komputer z agentem zostanie dodany do organizacji, czy do jednej z jednostek.
   Monit pojawia się w sytuacji, gdy administrujesz więcej niż jedną jednostką lub organizacją mającą co najmniej jedną jednostkę. W przeciwnym razie komputer zostanie dodany w trybie dyskretnym do administrowanej jednostki lub organizacji. Więcej informacji można znaleźć w sekcji "Jednostki i konta administracyjne" (s. 666).
9. [Opcjonalnie] Zmień inne ustawienia instalacji zgodnie z opisem podanym w sekcji "Dostosowywanie ustawień instalacji" (s. 88).
10. Kliknij **Zainstaluj**, aby kontynuować instalację.
11. Po zakończeniu instalacji kliknij **Zamknij**.
12. [Tylko w przypadku instalowania agenta dla VMware (Windows)] Wykonaj procedurę opisaną w sekcji "Konfigurowanie już zarejestrowanego agenta dla VMware" (s. 107).
13. [Tylko w przypadku instalowania agenta dla programu Exchange] Otwórz konsolę internetową Cyber Protect, kliknij **Dodaj** > **Microsoft Exchange Server** > **Skrzynki pocztowe programu Exchange**, a następnie wskaż komputer z włączoną rolą serwera **Dostęp klienta** programu Microsoft Exchange Server. Więcej informacji można znaleźć w sekcji "Kopia zapasowa skrzynki pocztowej" (s. 468).

Instalacja w systemie Linux

Przygotowanie

1. Upewnij się, że na komputerze są zainstalowane niezbędne pakiety systemu Linux.
2. Instalując agenta w systemie SUSE Linux, koniecznie użyj polecenia `su`, a nie `sudo`. Jeśli tego nie zrobisz, to przy próbie zarejestrowania agenta za pośrednictwem konsoli internetowej Cyber Protect wystąpi następujący błąd: `Nie udało się uruchomić przeglądarki internetowej. Brak dostępnego ekranu.`

   Niektóre dystrybucje systemu Linux, na przykład SUSE, nie analizują zmiennej `DISPLAY` w przypadku użycia polecenia `sudo` i instalator nie może otworzyć przeglądarki w graficznym interfejsie użytkownika (GUI).

Instalacja

Aby zainstalować agenta dla systemu Linux, potrzebujesz co najmniej 2 GB wolnego miejsca na dysku.

Aby zainstalować agenta dla systemu Linux

1. Jako użytkownik root przejdź do katalogu z plikiem instalacyjnym (.i686 lub .x86_64), zmień plik w plik wykonywalny, a następnie go uruchom.

   ```
   chmod +x <installation file name>
   ```

   ```
   ./<installation file name>
   ```

2. Zaakceptuj warunki umowy licencyjnej.
3. Wskaż komponenty do zainstalowania:
   a. Wyczyść pole wyboru **Acronis Cyber Protect Management Server**.
   b. Zaznacz pola wyboru odpowiadające agentom, które chcesz zainstalować. Dostępne są następujące agenty:
      - **Agent dla systemu Linux**
      - **Agent dla programu Oracle**

      Agent dla programu Oracle wymaga zainstalowania również agenta dla systemu Linux.
   c. Kliknij **Dalej**.
4. Określ serwer zarządzania, na którym zostanie zarejestrowany komputer z agentem:
   a. Określ nazwę hosta lub adresIP komputera, na którym jest zainstalowany serwer zarządzania.
   b. Podaj nazwę użytkownika i hasło administratora serwera zarządzania.
   c. Kliknij **Dalej**.

5. Jeśli pojawi się monit, wskaż, czy komputer z agentem zostanie dodany do organizacji, czy do jednej z jednostek, a następnie naciśnij **Enter**.
   Monit pojawia się w sytuacji, gdy konto określone w poprzednim kroku służy do administrowania więcej niż jedną jednostką lub organizacją mającą co najmniej jedną jednostkę.
6. Jeśli na komputerze jest włączona funkcja UEFI Secure Boot, pojawi się informacja o konieczności ponownego uruchomienia systemu po zakończeniu instalacji. Koniecznie zapamiętaj, jakiego hasła (hasła użytkownika root czy hasła „acronis") należy użyć.

   Uwaga
   Instalacja wygeneruje nowy klucz, który służy do podpisywania modułów jądra. Musisz zarejestrować ten nowy klucz na liście kluczy właściciela komputera przez ponowne uruchomienie komputera. Bez rejestracji nowego klucza agent nie będzie działać. Jeśli po instalacji agenta zostanie włączona funkcja UEFI Secure Boot, trzeba ponownie zainstalować agenta.

7. Po instalacji wykonaj jedną z następujących czynności:
   - Jeśli w ramach poprzedniego kroku pojawił się monit o ponowne uruchomienie systemu, kliknij **Uruchom ponownie**.
     Podczas ponownego uruchamiania systemu wybierz opcję zarządzania kluczem właściciela komputera, zaznacz **Zarejestruj klucz właściciela komputera**, a następnie zarejestruj klucz przy użyciu hasła zalecanego w poprzednim kroku.
   - W przeciwnym razie kliknij **Zakończ**.

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

Instalacja w systemie macOS

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**, a następnie kliknij **Kontynuuj**.
4. [Opcjonalnie] Kliknij **Zmień lokalizację instalacji**, aby zmienić dysk, na którym ma zostać zainstalowane oprogramowanie. Domyślnie wybrany jest dysk rozruchowy systemu.
5. Kliknij **Zainstaluj**. Jeśli pojawi się monit, podaj nazwę użytkownika i hasło administratora.
6. Określ serwer zarządzania, na którym zostanie zarejestrowany komputer z agentem:
   a. Określ nazwę hosta lub adresIP komputera, na którym jest zainstalowany serwer zarządzania.
   b. Podaj nazwę użytkownika i hasło administratora serwera zarządzania.
   c. Kliknij **Zarejestruj**.
7. Jeśli pojawi się monit, wskaż, czy komputer z agentem zostanie dodany do organizacji, czy do jednej z jednostek, a następnie kliknij **Gotowe**.

Monit pojawia się w sytuacji, gdy konto określone w poprzednim kroku służy do administrowania więcej niż jedną jednostką lub organizacją mającą co najmniej jedną jednostkę.

8. Po zakończeniu instalacji kliknij **Zamknij**.

Instalacja nienadzorowana lub dezinstalacja

Instalacja nienadzorowana lub dezinstalacja w systemie Windows

W tej sekcji opisano, jak zainstalować lub odinstalować agenty ochrony Acronis Cyber Protect w trybie nienadzorowanym na komputerze z systemem Windows za pomocą Instalatora Windows (programu `msiexec`). W domenie Active Directory instalację nienadzorowaną można wykonać również przy użyciu zasad grupy — zobacz "Wdrażanie agentów przy użyciu zasad grupy" (s. 182).

Podczas instalacji można skorzystać z tzw. **pliku transformacji** (pliku .mst). Plik transformacji zawiera parametry instalacji. Parametry instalacji można też określić bezpośrednio w wierszu polecenia.

Tworzenie transformacji .mst i wyodrębnianie pakietów instalacyjnych

1. Zaloguj się jako administrator i uruchom program instalacyjny.
2. Kliknij **Utwórz pliki .mst i .msi na potrzeby instalacji nienadzorowanej**.
3. [Opcja niedostępna w niektórych programach instalacyjnych] W polu **Bitowość komponentu** wybierz **32-bitowy** lub **64-bitowy**.
4. W polu **Elementy do zainstalowania** wybierz komponenty, które chcesz zainstalować, a następnie kliknij **Gotowe**.

   Z programu instalacyjnego zostaną wyodrębnione pakiety instalacyjne tych komponentów.
5. W oprogramowaniu **Acronis Cyber Protect Management Server** wybierz **Użyj poświadczeń** lub **Użyj tokenu rejestracji**. W zależności od wyboru określ poświadczenia lub token rejestracji, a następnie kliknij **Gotowe**.

   Dodatkowe informacje o procedurze generowania tokenu rejestracji można znaleźć w sekcji "Krok 1: Generowanie tokenu rejestracji" (s. 183).
6. [Tylko w przypadku instalowania na kontrolerze domeny] W obszarze **Konto logowania dla usługi agenta** wybierz **Użyj następującego konta**. Określ konto użytkownika, które będzie służyć do uruchamiania usługi agenta, a następnie kliknij **Gotowe**. Ze względów bezpieczeństwa program instalacyjny nie tworzy automatycznie nowych kont na kontrolerze domeny.

   Uwaga
   Wskazane konto użytkownika musi mieć przyznane prawo `Logowanie jako usługa`.
   Konto to musi już być używane na kontrolerze domeny, aby jego folder profilu został utworzony na tym komputerze.

   Dodatkowe informacje o instalowaniu agenta na kontrolerze domeny w trybie tylko do odczytu można znaleźć w tym artykule z bazy wiedzy Knowledge Base.

7. Przejrzyj lub zmodyfikuj inne ustawienia instalacji, które zostaną dodane do pliku .mst, a następnie kliknij **Kontynuuj**.
8. Wybierz folder, w którym zostanie wygenerowana transformacja .mst i zostaną wyodrębnione pakiety instalacyjne .msi i .cab, a następnie kliknij **Wygeneruj**.

W wyniku tego zostanie wygenerowany plik transformacji .mst, a do wskazanego folderu zostaną wyodrębnione pakiety instalacyjne .msi oraz .cab.

Instalowanie programu przy użyciu pliku transformacji .mst

W wierszu polecenia uruchom następujące polecenie:

```
msiexec /i <package name> TRANSFORMS=<transform name>
```

Gdzie:

- `<nazwa pakietu>` oznacza nazwę pliku .msi. Nazwa ta to **AB.msi** lub **AB64.msi**, w zależności od bitowości systemu operacyjnego.
- `<nazwa przekształcenia>` oznacza nazwę transformacji. Nazwa ta to **AB.msi.mst** lub **AB64.msi.mst**, w zależności od bitowości systemu operacyjnego.

Na przykład `msiexec /i AB64.msi TRANSFORMS=AB64.msi.mst`

Instalowanie lub odinstalowywanie programu przez ręczne określenie parametrów

W wierszu polecenia uruchom następujące polecenie:

```
msiexec /i <package name><PARAMETER 1>=<value 1> ... <PARAMETER N>=<value n>
```

`<nazwa pakietu>` oznacza tu nazwę pliku .msi. Nazwa ta to **AB.msi** lub **AB64.msi**, w zależności od bitowości systemu operacyjnego.

Dostępne parametry i ich wartości opisano w sekcji "Parametry wspólne" (s. 114).

Przykłady

- Instalowanie serwera zarządzania i komponentów do instalacji zdalnej.

  ```
  msiexec.exe /i ab64.msi /l*v my_log.txt /qn
  ADDLOCAL=AcronisCentralizedManagementServer,WebConsole,ComponentRegisterFeature
  TARGETDIR="C:\Program Files\Acronis" REBOOT=ReallySuppress CURRENT_LANGUAGE=en ACEP_
  AGREEMENT=1 AMS_USE_SYSTEM_ACCOUNT=1
  ```

- Instalowanie agenta dla systemu Windows, narzędzia wiersza polecenia i narzędzia Cyber Protect Monitor. Rejestrowanie komputera z agentem na wcześniej zainstalowanym serwerze zarządzania.

  ```
  msiexec.exe /i ab64.msi /l*v my_log.txt /qn
  ADDLOCAL=AgentsCoreComponents,BackupAndRecoveryAgent,CommandLineTool,TrayMonitor
  ```

```
TARGETDIR="C:\Program Files\Acronis" REBOOT=ReallySuppress CURRENT_LANGUAGE=en ACEP_
AGREEMENT=1 MMS_CREATE_NEW_ACCOUNT=1 REGISTRATION_ADDRESS=10.10.1.1
```

- Aktualizowanie serwera zarządzania, węzła magazynowania, usługi wykazu i agenta ochrony.

```
msiexec.exe /i ab64.msi /l*v my_log.txt /qn
ADDLOCAL=AcronisCentralizedManagementServer,BackupAndRecoveryAgent,AgentsCoreComponen
ts,StorageServer,CatalogBrowser CATALOG_DATA_MIGRATION_PATH="C:\MyFolder\tmp"
```

Parametry instalacji nienadzorowanej lub dezinstalacji

W tej sekcji opisano parametry używane podczas instalacji nienadzorowanej lub dezinstalacji w systemie Windows.

Oprócz tych parametrów można tez używać innych parametrów programu `msiexec` zgodnie z opisem podanym w artykule https://msdn.microsoft.com/en-us/library/windows/desktop/aa367988(v=vs.85).aspx.

Parametry instalacji

Parametry wspólne

`ADDLOCAL=<list of components>`

Nazwy komponentów do zainstalowania, rozdzielone przecinkami bez spacji. Przed instalacją należy wyodrębnić z programu instalacyjnego wszystkie wskazane komponenty.

Oto pełna lista komponentów:

Komponent	Inne wymagane równolegle komponenty	Bitowość	Nazwa/opis komponentu
AcronisCentralizedManagementServer	WebConsole	wersja 32-bitowa/64-bitowa	Serwer zarządzania
WebConsole	AcronisCentralizedManagementServer	wersja 32-bitowa/64-bitowa	Web Console
ComponentRegisterFeature	AcronisCentralizedManagementServer	wersja 32-bitowa/64-bitowa	Komponenty do instalacji zdalnej
AtpScanService	AcronisCentralizedManagementServer	wersja 32-bitowa/64-bitowa	Usługa Skanowanie
AgentsCoreComponents		wersja 32-	Podstawowe

		bitowa/64-bitowa	komponenty dla agentów
BackupAndRecoveryAgent	AgentsCoreComponents	wersja 32-bitowa/64-bitowa	Agent dla systemu Windows
ArxAgentFeature	BackupAndRecoveryAgent	wersja 32-bitowa/64-bitowa	Agent dla programu Exchange
ArsAgentFeature	BackupAndRecoveryAgent	wersja 32-bitowa/64-bitowa	Agent dla SQL
ARADAgentFeature	BackupAndRecoveryAgent	wersja 32-bitowa/64-bitowa	Agent dla usługi Active Directory
OracleAgentFeature	BackupAndRecoveryAgent	wersja 32-bitowa/64-bitowa	Agent dla programu Oracle
ArxOnlineAgentFeature	AgentsCoreComponents	wersja 32-bitowa/64-bitowa	Agent dla usługi Office 365
AcronisESXSupport	AgentsCoreComponents	wersja 32-bitowa/64-bitowa	Agent dla VMware (Windows)
HyperVAgent	AgentsCoreComponents	wersja 32-bitowa/64-bitowa	Agent dla Hyper-V
ESXVirtualAppliance		wersja 32-bitowa/64-bitowa	Agent dla VMware (urządzenie wirtualne)
ScaleVirtualAppliance		wersja 32-bitowa/64-bitowa	Agent dla Scale Computing HC3 (urządzenie wirtualne)
CommandLineTool		wersja 32-	Narzędzie

		bitowa/64-bitowa	wiersza polecenia
TrayMonitor	BackupAndRecoveryAgent	wersja 32-bitowa/64-bitowa	Cyber Protect Monitor
BackupAndRecoveryBootableComponents		wersja 32-bitowa/64-bitowa	Generator nośnika startowego
PXEServer		wersja 32-bitowa/64-bitowa	Serwer PXE
StorageServer	BackupAndRecoveryAgent	64-bitowy	Węzeł magazynowania
CatalogBrowser	JRE 8 Update 111 lub nowsze	64-bitowy	Usługa wykazu

`TARGETDIR=<path>`

Folder, w którym chcesz zainstalować program.

`REBOOT=ReallySuppress`

W przypadku określenia tego parametru ponowny rozruch komputera jest wzbroniony.

`CURRENT_LANGUAGE=<language ID>`

Język programu. Dostępne są następujące wartości: `en`, `en_GB`, `cs`, `da`, `de`, `es_ES`, `fr`, `ko`, `it`, `hu`, `nl`, `ja`, `pl`, `pt`, `pt_BR`, `ru`, `tr`, `zh`, `zh_TW`.

`ACEP_AGREEMENT={0,1}`

W przypadku wartości `1` komputer zostanie objęty Programem jakości obsługi klienta firmy Acronis (ACEP).

`REGISTRATION_ADDRESS=<host name or IP address>:<port>`

Nazwa hosta lub adres IP komputera, na którym jest zainstalowany serwer zarządzania. Agenty, węzeł magazynowania i usługa wykazu określone w parametrze `ADDLOCAL` zostaną zarejestrowane na tym serwerze zarządzania. Jeśli numer portu jest inny niż wartość domyślna (9877), trzeba go podać.

Za pomocą tego parametru trzeba określić parametr `REGISTRATION_TOKEN` lub parametry `REGISTRATION_LOGIN` i `REGISTRATION_PASSWORD`.

`REGISTRATION_TOKEN=<token>`

Token rejestracji wygenerowany w konsoli internetowej Cyber Protect zgodnie z opisem podanym w sekcji Wdrażanie agentów przy użyciu zasad grupy.

`REGISTRATION_LOGIN=<user name>, REGISTRATION_PASSWORD=<password>`

Nazwa użytkownika i hasło administratora serwera zarządzania.

`REGISTRATION_TENANT=<unit ID>`

Jednostka w ramach organizacji. Agenty, węzeł magazynowania i usługa wykazu określone w parametrze `ADDLOCAL` zostaną dodane do tej jednostki.

Aby poznać identyfikator jednostki, w konsoli internetowej Cyber Protect kliknij **Ustawienia** > **Konta**, wybierz jednostkę i kliknij **Szczegóły**.

Ten parametr nie działa bez parametrów `REGISTRATION_TOKEN` lub `REGISTRATION_LOGIN` i `REGISTRATION_PASSWORD`. W takim przypadku komponenty zostaną dodane do organizacji.

W przypadku nieokreślenia tego parametru komponenty zostaną dodane do organizacji.

`REGISTRATION_REQUIRED={0,1}`

Wynik instalacji w razie niepowodzenia rejestracji. W przypadku wartości `1` instalacja się nie powiedzie. W przypadku wartości `0` instalacja przebiegnie pomyślnie, mimo że komponent nie został zarejestrowany.

`REGISTRATION_CA_SYSTEM={0,1}|REGISTRATION_CA_BUNDLE={0,1}|REGISTRATION_PINNED_PUBLIC_KEY=<public key value>`

Te wzajemnie się wykluczające parametry umożliwiają określenie metody sprawdzania certyfikatu serwera zarządzania podczas rejestracji. Sprawdzenie certyfikatu pozwala zweryfikować autentyczność serwera zarządzania w celu zapobieżenia atakom MITM.

W przypadku wartości `1` do weryfikacji jest używany odpowiednio urząd certyfikacji systemu lub pakiet urzędu certyfikacji dostarczony wraz z produktem. W przypadku podania przypiętego klucza publicznego do weryfikacji jest używany ten klucz. W przypadku wartości `0` lub nieokreślenia tych parametrów weryfikacja certyfikatu jest pomijana, ale ruch związany z rejestracją pozostaje szyfrowany.

`/l*v <log file>`

W przypadku określenia tego parametru we wskazanym pliku zostanie zapisany dziennik instalacji w trybie informacji pełnej. Pliku dziennika można użyć do analizowania problemów z instalacją.

Parametry instalacji serwera zarządzania

`WEB_SERVER_PORT=<port number>`

Port, którego przeglądarka internetowa będzie używać w celu uzyskania dostępu do serwera zarządzania. Domyślnie jest to port 9877.

`AMS_ZMQ_PORT=<port number>`

Port, który będzie używany do komunikacji między komponentami programu. Domyślnie jest to port 7780.

`SQL_INSTANCE=<instance>`

Baza danych, która będzie używana przez serwer zarządzania. Możesz wybrać dowolną wersję programu Microsoft SQL Server 2012, Microsoft SQL Server 2014 lub Microsoft SQL Server 2016. Wybrana instancja może być również używana przez inne programy.

W przypadku nieokreślenia tego parametru będzie używana wbudowana baza danych SQLite.

`SQL_USER_NAME=<user name>` i `SQL_PASSWORD=<password>`

Poświadczenia konta logowania do programu Microsoft SQL Server. Serwer zarządzania będzie używać tych poświadczeń do nawiązywania połączeń z wybraną instancją serwera SQL. W przypadku nieokreślenia tych parametrów serwer zarządzania będzie używać poświadczeń konta usługi serwera zarządzania (**AMS User**).

Konto, na którym będzie działać usługa serwera zarządzania

Określ jeden z następujących parametrów:

- `AMS_USE_SYSTEM_ACCOUNT={0,1}`
  W przypadku wartości `1` będzie używane konto systemowe.
- `AMS_CREATE_NEW_ACCOUNT={0,1}`
  W przypadku wartości `1` zostanie utworzone nowe konto.
- `AMS_SERVICE_USERNAME=<user name>` i `AMS_SERVICE_PASSWORD=<password>`
  Będzie używane wskazane konto.

Parametry instalacji agenta

`HTTP_PROXY_ADDRESS=<IP address>` i `HTTP_PROXY_PORT=<port>`

Serwer proxy HTTP, którego ma używać agent. W przypadku nieokreślenia tych parametrów serwer proxy nie będzie używany.

`HTTP_PROXY_LOGIN=<login>` i `HTTP_PROXY_PASSWORD=<password>`

Poświadczenia dostępu do serwera proxy HTTP. Jeśli serwer wymaga uwierzytelniania, należy użyć tych parametrów.

`HTTP_PROXY_ONLINE_BACKUP={0,1}`

W przypadku wartości `0` lub nieokreślenia tego parametru agent użyje serwera proxy tylko w przypadku tworzenia kopii zapasowej i odzyskiwania z chmury. W przypadku wartości `1` agent również połączy się z serwerem zarządzania za pośrednictwem serwera proxy.

`SET_ESX_SERVER={0,1}`

W przypadku wartości `0` nie będzie ustanawiane połączenie między instalowanym agentem dla VMware a serwerem vCenter lub hostem ESXi. Po instalacji postępuj zgodnie z opisem podanym w sekcji „Konfigurowanie już zarejestrowanego agenta dla VMware”.

W przypadku wartości `1` określ następujące parametry:

`ESX_HOST=<host name or IP address>`

Nazwa hosta lub adres IP serwera vCenter lub hosta ESXi.

`ESX_USER=<user name>` i `ESX_PASSWORD=<password>`

Poświadczenia dostępu do serwera vCenter lub hosta ESXi.

Konto, na którym będzie działać usługa agenta

Określ jeden z następujących parametrów:

- `MMS_USE_SYSTEM_ACCOUNT={0,1}`
  W przypadku wartości `1` będzie używane konto systemowe.
- `MMS_CREATE_NEW_ACCOUNT={0,1}`
  W przypadku wartości `1` zostanie utworzone nowe konto.
- `MMS_SERVICE_USERNAME=<user name>` i `MMS_SERVICE_PASSWORD=<password>`
  Będzie używane wskazane konto.

Parametry instalacji węzła magazynowania

Konto, na którym będzie działać usługa węzła magazynowania

Określ jeden z następujących parametrów:

- `ASN_USE_SYSTEM_ACCOUNT={0,1}`
  W przypadku wartości `1` będzie używane konto systemowe.
- `ASN_CREATE_NEW_ACCOUNT={0,1}`
  W przypadku wartości `1` zostanie utworzone nowe konto.
- `ASN_SERVICE_USERNAME=<user name>` i `ASN_SERVICE_PASSWORD=<password>`
  Będzie używane wskazane konto.

Parametry instalacji usługi wykazu

`CATALOG_DATA_MIGRATION_PATH=<path>`

Używając tego parametru, można przeprowadzić migrację danych wykazu do nowej wersji usługi wykazu w rozwiązaniu Acronis Cyber Protect 15 Update 4. Określ ścieżkę do folderu tymczasowego, do którego zostaną wyeksportowane dane wykazu.

`SKIP_CATALOG_DATA_MIGRATION=1`

Za pomocą tego parametru można pominąć migrację danych wykazu.

Parametry `SKIP_CATALOG_DATA_MIGRATION` i `CATALOG_DATA_MIGRATION_PATH` wykluczają się wzajemnie.

Parametry dezinstalacji

`REMOVE={<list of components>|ALL}`

Nazwy komponentów do usunięcia, rozdzielone przecinkami bez spacji.

Dostępne komponenty opisano wcześniej w tej sekcji.

W przypadku wartości `ALL` zostaną odinstalowane wszystkie komponenty produktu. Ponadto można określić następujący parametr:

`DELETE_ALL_SETTINGS={0, 1}`

W przypadku wartości `1` dzienniki, zadania i ustawienia konfiguracji programu zostaną usunięte.

Instalacja nienadzorowana lub dezinstalacja w systemie Linux

W tej sekcji opisano, jak zainstalować lub odinstalować program Acronis Cyber Protect w trybie nienadzorowanym na komputerze z systemem Linux przy użyciu wiersza polecenia.

Aby zainstalować lub odinstalować program

1. Otwórz terminal.
2. Uruchom następujące polecenie:

   ```
   <package name> -a <parameter 1> ... <parameter N>
   ```

   Zmienna `<nazwa pakietu>` oznacza nazwę pakietu instalacyjnego (pliku .i686 lub .x86_64)
3. [Tylko w przypadku instalowania agenta dla systemu Linux] Jeśli na komputerze jest włączona funkcja UEFI Secure Boot, po zakończeniu instalacji pojawi się komunikat o konieczności ponownego uruchomienia systemu. Koniecznie zapamiętaj, jakiego hasła (hasła użytkownika root czy hasła „acronis”) należy użyć. Podczas ponownego uruchamiania systemu wybierz opcję zarządzania kluczem właściciela komputera, zaznacz **Zarejestruj klucz właściciela komputera**, a następnie zarejestruj klucz przy użyciu zalecanego hasła.

Jeśli po instalacji agenta zostanie włączona funkcja UEFI Secure Boot, powtórz instalację, w tym krok 3. W przeciwnym razie następne operacje tworzenia kopii zapasowej zakończą się niepowodzeniem.

Parametry instalacji

Parametry wspólne

`{-i |--id=}<list of components>`

Nazwy komponentów do zainstalowania, rozdzielone przecinkami bez spacji.

Dostępne są następujące komponenty do zainstalowania:

Komponent	Opis komponentu
AcronisCentralizedManagementServer	Serwer zarządzania
BackupAndRecoveryAgent	Agent dla systemu Linux
BackupAndRecoveryBootableComponents	Generator nośnika startowego

W przypadku nieokreślenia tego parametru zostaną zainstalowane wszystkie powyższe komponenty.

`--language=<language ID>`

Język programu. Dostępne są następujące wartości: `en`, `en_GB`, `cs`, `da`, `de`, `es_ES`, `fr`, `ko`, `it`, `hu`, `nl`, `ja`, `pl`, `pt`, `pt_BR`, `ru`, `tr`, `zh`, `zh_TW`.

`{-d|--debug}`

W przypadku określenia tego parametru dziennik instalacji zostanie zapisany w trybie informacji pełnej. Dziennik znajduje się w pliku **/var/log/trueimage-setup.log**.

`{-t|--strict}`

W przypadku określenia tego parametru wystąpienie ostrzeżenia podczas instalacji poskutkuje niepowodzeniem instalacji. W przypadku nieokreślenia tego parametru instalacja zostanie pomyślnie ukończona nawet w razie wystąpienia ostrzeżeń.

`{-n|--nodeps}`

W przypadku określenia tego parametru brak wymaganych pakietów systemu Linux zostanie zignorowany podczas instalacji.

Parametry instalacji serwera zarządzania

`{-W |--web-server-port=}<port number>`

Port, którego przeglądarka internetowa będzie używać w celu uzyskania dostępu do serwera zarządzania. Domyślnie jest to port 9877.

`--ams-tcp-port=<port number>`

Port, który będzie używany do komunikacji między komponentami programu. Domyślnie jest to port 7780.

Parametry instalacji agenta

Określ jeden z następujących parametrów:

- `--skip-registration`
  - Pominięcie rejestracji agenta na serwerze zarządzania.
- `{-C |--ams=}<host name or IP address>`

- Nazwa hosta lub adres IP komputera, na którym jest zainstalowany serwer zarządzania. Agent zostanie zarejestrowany na tym serwerze zarządzania.

  Jeśli zainstalujesz agenta i serwer zarządzania za pomocą jednego polecenia, agent zostanie zarejestrowany na tym serwerze zarządzania mimo parametru `-C`.

  Za pomocą tego parametru trzeba określić parametr `token` lub parametry `login` i `password`.

  `--token=<token>`

  Token rejestracji wygenerowany w konsoli internetowej Cyber Protect zgodnie z opisem podanym w sekcji Wdrażanie agentów przy użyciu zasad grupy.

  `{-g |--login=}<user name>` i `{-w |--password=}<password>`

  Poświadczenia administratora serwera zarządzania.

  `--unit=<unit ID>`

  Jednostka w ramach organizacji. Agent zostanie dodany do tej jednostki.

  Aby poznać identyfikator jednostki, w konsoli internetowej Cyber Protect kliknij **Ustawienia** > **Konta**, wybierz jednostkę i kliknij **Szczegóły**.

  W przypadku nieokreślenia tego parametru agent zostanie dodany do organizacji.

  `--reg-transport={https|https-ca-system|https-ca-bundle|https-pinned-public-key}`

  Metoda sprawdzania certyfikatu serwera zarządzania podczas rejestracji. Sprawdzenie certyfikatu pozwala zweryfikować autentyczność serwera zarządzania w celu zapobieżenia atakom MITM.

  W przypadku wartości `https` lub nieokreślenia parametru sprawdzanie certyfikatu jest pomijane, ale ruch związany z rejestracją pozostaje szyfrowany. W przypadku wartości *innej niż* `https` do sprawdzenia jest używany odpowiednio urząd certyfikacji systemu, pakiet urzędu certyfikacji dostarczony wraz z produktem lub przypięty klucz publiczny.

  `--reg-transport-pinned-public-key=<public key value>`

  Wartość przypiętego klucza publicznego. Ten parametr należy określić wraz z parametrem `--reg-transport=https-pinned-public-key`.

- `--http-proxy-host=<IP address>` i `--http-proxy-port=<port>`
  - Serwer proxy HTTP, którego agent będzie używać do tworzenia kopii zapasowych lub odzyskiwania z chmury i nawiązywania połączenia z serwerem zarządzania. W przypadku nieokreślenia tych parametrów serwer proxy nie będzie używany.
- `--http-proxy-login=<login>` i `--http-proxy-password=<password>`
  - Poświadczenia dostępu do serwera proxy HTTP. Jeśli serwer wymaga uwierzytelniania, należy użyć tych parametrów.

- `--no-proxy-to-ams`
  - Agent ochrony połączy się z serwerem zarządzania bez użycia serwera proxy określonego przy użyciu parametrów `--http-proxy-host` i `--http-proxy-port`.

Parametry dezinstalacji

`{-u|--uninstall}`

Powoduje dezinstalację programu.

`--purge`

Powoduje usunięcie dzienników, zadań i ustawień konfiguracyjnych programu.

Parametry informacyjne

`{-?|--help}`

Umożliwia wyświetlenie opisu parametrów.

`--usage`

Umożliwia wyświetlenie krótkiego opisu zastosowań polecenia.

`{-v|--version}`

Umożliwia wyświetlenie wersji pakietu instalacyjnego.

`--product-info`

Umożliwia wyświetlenie nazwy produktu i wersji pakietu instalacyjnego.

Przykłady

- Instalowanie serwera zarządzania.

```
./AcronisCyberProtect_15_64-bit.x86_64 -a -i AcronisCentralizedManagementServer
```

- Instalowanie serwera zarządzania z określeniem niestandardowych portów.

```
./AcronisCyberProtect_15_64-bit.x86_64 -a -i AcronisCentralizedManagementServer --
web-server-port 6543 --ams-tcp-port 8123
```

- Instalowanie agenta dla systemu Linux i rejestrowanie go na wskazanym serwerze zarządzania.

```
./AcronisCyberProtect_15_64-bit.x86_64 -a -i BackupAndRecoveryAgent --ams 10.10.1.1 -
-login root --password 123456
```

- Instalowanie agenta dla systemu Linux i rejestrowanie go na wskazanym serwerze zarządzania we wskazanej jednostce.

```
./AcronisCyberProtect_15_64-bit.x86_64 -a -i BackupAndRecoveryAgent --ams 10.10.1.1 -
-login root --password 123456 -unit 01234567-89AB-CDEF-0123-456789ABCDEF
```

Instalacja nienadzorowana lub dezinstalacja w systemie macOS

W tej sekcji opisano, jak zainstalować, zarejestrować i odinstalować agenta ochrony w trybie nienadzorowanym na komputerze z systemem macOS przy użyciu wiersza polecenia. Informacje na temat pobierania pliku instalacyjnego (.dmg) można znaleźć w sekcji „Dodawanie komputera z systemem macOS”.

Aby zainstalować agenta dla systemu Mac

1. Utwórz tymczasowy katalog, w którym zamontujesz plik instalacyjny (.dmg).

   ```
   mkdir <dmg_root>
   ```

   Tutaj `<katalog_główny_dmg>` oznacza dowolną odpowiadającą Ci nazwę.
2. Zamontuj plik .dmg.

   ```
   hdiutil attach <dmg_file> -mountpoint <dmg_root>
   ```

   Tutaj `<plik_dmg>` oznacza nazwę pliku instalacyjnego. Na przykład **AcronisCyberProtect_15_MAC.dmg**.
3. Uruchom instalator.

   ```
   sudo installer -pkg <dmg_root>/Install.pkg -target LocalSystem
   ```
4. Odmontuj plik instalacyjny (.dmg).

   ```
   hdiutil detach <dmg_root>
   ```

Przykłady

- ```
  mkdir mydirectory
  ```

  ```
  hdiutil attach /Users/JohnDoe/AcronisCyberProtect_15_MAC.dmg -mountpoint mydirectory
  ```

  ```
  sudo installer -pkg mydirectory/Install.pkg -target LocalSystem
  ```

  ```
  hdiutil detach mydirectory
  ```

Aby zarejestrować agenta dla systemu Mac

Wykonaj jedną z następujących czynności:

- Zarejestruj agenta w ramach określonego konta administratora.
  ```

```
sudo /Library/Application\
Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent -o register -a
<management server address:port> -u <user name> -p <password>
```

Zmienna `<adres:port serwera zarządzania>` oznacza nazwę hosta lub adres IP komputera, na którym jest instalowany moduł Acronis Cyber Protect Management Server. Jeśli numer portu jest inny niż domyślny (9877), trzeba go podać.

Zmienne `<nazwa użytkownika>` i `<hasło>` oznaczają poświadczenia dostępu do konta administratora, w ramach którego zostanie zarejestrowany agent.

- Zarejestruj agenta w określonej jednostce.

```
sudo /Library/Application\
Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent  -o register -a
<management server address:port> -u <user name> -p <password> --tenant <unit ID>
```

Aby poznać identyfikator jednostki, w konsoli internetowej Cyber Protect kliknij **Ustawienia** > **Konta**, zaznacz odpowiednią jednostkę i kliknij **Szczegóły**.

Ważne
Administratorzy mogą rejestrować agenty przez podanie identyfikatora jednostki wyłącznie na własnym poziomie hierarchii organizacji. Administratorzy jednostek mogą rejestrować komputery we własnych jednostkach i ich jednostkach podrzędnych. Administratorzy organizacji mogą rejestrować komputery we wszystkich jednostkach. Więcej informacji na temat różnych kont administratorów można znaleźć w sekcji „Administrowanie kontami użytkowników i jednostkami organizacyjnymi”.

- Zarejestruj agenta przy użyciu tokenu rejestracji.

```
sudo /Library/Application\
Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent -o register -a
<management server address:port> --token <token>
```

Token rejestracji to ciąg 12 znaków podzielony dywizami na trzy części. Można go wygenerować w konsoli internetowej Cyber Protect zgodnie z instrukcją podaną w sekcji „Wdrażanie agentów przy użyciu zasad grupy”.

Ważne
W systemie macOS 10.14 lub nowszym trzeba przyznać agentowi ochrony pełny dostęp do dysku. W tym celu przejdź do sekcji **Aplikacje** > **Narzędzia** i uruchom program **Asystent agenta Cyber Protect Agent**. Następnie postępuj zgodnie z instrukcjami wyświetlanymi w oknie aplikacji.

Przykłady

Rejestracja przy użyciu nazwy użytkownika i hasła.

- ```
  sudo /Library/Application\
  Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent -o register -a
  https://10.250.144.179:9877 -u johndoe -p johnspassword
  ```

Rejestracja przy użyciu identyfikatora jednostki i poświadczeń administratora.

- ```
  sudo /Library/Application\
  Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent -o register -a
  https://10.250.144.179:9877 -u johndoe -p johnspassword --tenant 4dd941c1-c03f-11ea-
  86d8-005056bdd3a0
  ```

Rejestracja przy użyciu tokenu.

- ```
  sudo /Library/Application\
  Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent -o register -a
  https://10.250.144.179:9877 --token D91D-DC46-4F0B
  ```

Aby odinstalować agenta dla systemu Mac

Uruchom następujące polecenie:

- ```
  sudo /Library/Application\ Support/BackupClient/Acronis/Cyber\ Protect\ Agent\
  Uninstall.app/Contents/MacOS/AgentUninstall /confirm
  ```

Aby odinstalować agenta dla systemu Mac i usunąć wszystkie dzienniki, zadania oraz ustawienia konfiguracyjne, uruchom następujące polecenie:

- ```
  sudo /Library/Application\ Support/BackupClient/Acronis/Cyber\ Protect\ Agent\
  Uninstall.app/Contents/MacOS/AgentUninstall /confirm /purge
  ```

Ręczne rejestrowanie komputerów

Komputer można zarejestrować na serwerze zarządzania Cyber Protect nie tylko w ramach instalacji agenta, ale i przy użyciu interfejsu wiersza polecenia. Może to być konieczne, jeśli agent został zainstalowany, ale na przykład automatyczna rejestracja się nie powiodła lub chcesz zarejestrować istniejący już komputer na nowym koncie.

Aby zarejestrować komputer

W wierszu polecenia komputera, na którym zainstalowany jest agent, uruchom jedno z poniższych poleceń:

- Zarejestruj komputer w ramach określonego konta administratora:

  ```
  <path to the registration tool> -o register –a <management server address:port> -u
  <user name> -p <password>
  ```

  Zmienna `<ścieżka do narzędzia do rejestracji>` oznacza następującą ścieżkę:
  ```

- W systemie Windows: `%ProgramFiles%\Acronis\RegisterAgentTool\register_agent.exe`
- W systemie Linux: `/usr/lib/Acronis/RegisterAgentTool/RegisterAgent`
- W systemie macOS: `/Library/Application Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent`

Zmienna `<adres:port serwera zarządzania>` oznacza nazwę hosta lub adres IP komputera, na którym jest instalowany moduł Acronis Cyber Protect Management Server. Jeśli korzystasz z portu domyślnego 9877, nie musisz go podawać.

Zmienne `<nazwa użytkownika>` i `<hasło>` oznaczają poświadczenia dostępu do konta administratora, w ramach którego zostanie zarejestrowany agent.

- Aby zarejestrować komputer w określonej jednostce, podaj jej identyfikator:

```
<path to the registration tool> -o register -a <management server address:port> u
<user name> -p <password> --tenant <unit ID>
```

Aby poznać identyfikator jednostki, w konsoli internetowej Cyber Protect kliknij **Ustawienia** > **Konta**, zaznacz odpowiednią jednostkę i kliknij **Szczegóły**.

Ważne
Administratorzy mogą rejestrować agenty wyłącznie na własnym poziomie hierarchii organizacji. Administratorzy jednostek mogą rejestrować agenty we własnych jednostkach i ich jednostkach podrzędnych. Administratorzy organizacji mogą rejestrować agenty we wszystkich jednostkach. Więcej informacji na temat różnych kont administratorów można znaleźć w sekcji „Administrowanie kontami użytkowników i jednostkami organizacyjnymi”.

- Aby zarejestrować komputer przy użyciu tokenu rejestracji:

```
<path to the registration tool> -o register -a <management server address:port> --
token <token>
```

  - Token rejestracji to ciąg 12 znaków podzielony dywizami na trzy części. Więcej informacji o procedurze generowania tokenu można znaleźć w sekcji „Wdrażanie agentów przy użyciu zasad grupy”.

Aby wyrejestrować komputer

W wierszu polecenia komputera, na którym jest zainstalowany agent, uruchom polecenie:

```
<path to the registration tool> -o unregister
```

Przykłady

Windows

```
"%ProgramFiles%\Acronis\RegisterAgentTool\register_agent.exe" -o register -a
https://10.250.144.179:9877 -u johndoe -p johnspassword
```

```
"%ProgramFiles%\Acronis\RegisterAgentTool\register_agent.exe" -o register -a
https://10.250.144.179:9877 --tenant 590b1dd7-8adb-11ea-bf44-0050569deecf
```

```
"%ProgramFiles%\Acronis\RegisterAgentTool\register_agent.exe" -o register -a
https://10.250.144.179:9877 -u johndoe -p johnspassword --tenant 590b1dd7-8adb-11ea-
bf44-0050569deecf
```

```
"%ProgramFiles%\Acronis\RegisterAgentTool\register_agent.exe" -o register -a
https://10.250.144.179:9877 --token 3B4C-E967-4FBD
```

```
"%ProgramFiles%\Acronis\RegisterAgentTool\register_agent.exe" -o unregister
```

Linux

```
sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o register -a
https://10.250.144.179:9877 -u johndoe -p johnspassword
```

```
sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o register -a
https://10.250.144.179:9877 --tenant 590b1dd7-8adb-11ea-bf44-0050569deecf
```

```
sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o register -a
https://10.250.144.179:9877 -u johndoe -p johnspassword --tenant 590b1dd7-8adb-11ea-
bf44-0050569deecf
```

```
sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o register -a
https://10.250.144.179:9877 --token 34F6-8C39-4A5C
```

```
sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o unregister
```

macOS

```
sudo "/Library/Application Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent"
-o register -a https://10.250.144.179:9877 -u johndoe -p johnspassword
```

```
sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o register -a
https://10.250.144.179:9877 --tenant 590b1dd7-8adb-11ea-bf44-0050569deecf
```

```
sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o register -a
https://10.250.144.179:9877 -u johndoe -p johnspassword --tenant 590b1dd7-8adb-11ea-
bf44-0050569deecf
```

```
sudo "/Library/Application Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent"
-o register -a https://10.250.144.179:9877 --token 9DBF-3DA9-4DAB
```

```
sudo "/Library/Application Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent"
-o unregister
```

Hasła ze znakami specjalnymi lub spacjami

Jeśli Twoje hasło zawiera znaki specjalne lub spacje, wpisując je w wierszu polecenia, ujmij je w cudzysłów:

```
<path to the registration tool> -o register -a <management server address:port> -u <user
name> -p <"password">
```

Przykład (dotyczący systemu Windows):

```
"%ProgramFiles%\BackupClient\RegisterAgentTool\register_agent.exe" -o register -a
https://10.250.144.179:9877 -u johndoe -p "johns password"
```

Jeśli nadal pojawia się komunikat o błędzie:

1. Zakoduj hasło w formacie base64 na stronie https://www.base64encode.org/.
2. W wierszu polecenia podaj zakodowane hasło, używając parametru -b lub --base64.

Przykład (dotyczący systemu Windows):

```
"%ProgramFiles%\BackupClient\RegisterAgentTool\register_agent.exe" -o register -a
https://10.250.144.179:9877 -u johndoe -b -p am9obnNwYXNzd29yZA==
```

Sprawdzanie dostępności aktualizacji

Ta funkcja jest dostępna tylko dla administratorów organizacji.

Za każdym razem, gdy logujesz się do konsoli internetowej Cyber Protect, program Acronis Cyber Protect sprawdza dostępność nowej wersji w witrynie internetowej firmy Acronis. Jeśli nowa wersja jest dostępna, konsola internetowa Cyber Protect udostępni do niej łącze u dołu każdej strony na kartach **Urządzenia**, **Plany** i **Magazyn kopii zapasowych**. Łącze jest też dostępne na stronie **Ustawienia** > **Agenci**.

Aby włączyć lub wyłączyć automatyczne sprawdzanie dostępności aktualizacji, zmień ustawienie systemowe **Aktualizacje**.

Aby ręcznie sprawdzić dostępność aktualizacji, kliknij ikonę ze znakiem zapytania w prawym górnym rogu > **Informacje** > **Sprawdź dostępność aktualizacji** lub ikonę ze znakiem zapytania > **Sprawdź dostępność aktualizacji**.

Migrowanie serwera zarządzania

Serwer zarządzania działający na komputerze z systemem Windows można migrować na inny komputer z systemem Windows w tym samym środowisku.

Proces migracji obejmuje następujące fazy:

1. "Operacje na komputerze źródłowym" (s. 130)
   W tej fazie dane na pierwotnym serwerze zarządzania są przygotowywane do migracji.
2. "Operacje na komputerze docelowym" (s. 131)
   W tej fazie instaluje się i konfiguruje nowy serwer zarządzania, a następnie kopiuje dane z pierwotnego serwera zarządzania na nowy.

Wymagania wstępne

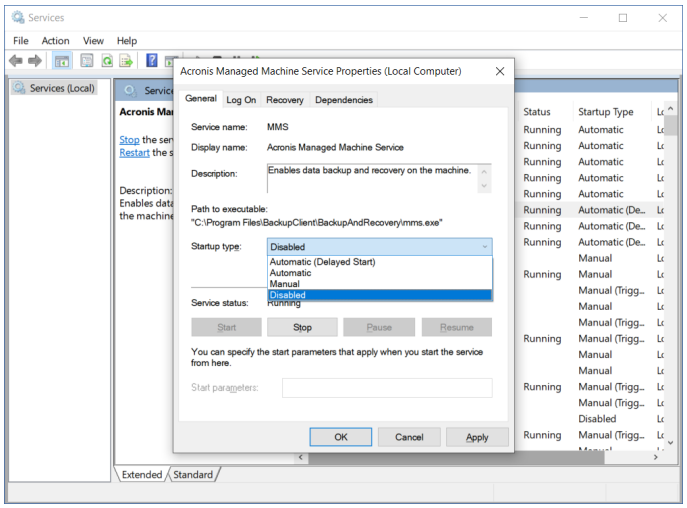
- Serwer zarządzania korzysta z zewnętrznej bazy danych programu Microsoft SQL Server. Instancja programu Microsoft SQL Server działa na komputerze docelowym.
- Agenty ochrony są zarejestrowane na serwerze zarządzania przy użyciu nazwy hosta, a nie adresu IP.
- Serwer zarządzania jest w wersji Acronis Cyber Protect Update 4 (kompilacja 29486) lub nowszej.
- Na komputerze źródłowym i docelowym jest zainstalowana ta sama wersja serwera zarządzania.

Operacje na komputerze źródłowym

W tej fazie dane z pierwotnego serwera zarządzania są przygotowywane do migracji.

Aby przygotować dane do migracji

1. Na pierwotnym komputerze serwera zarządzania zatrzymaj wszystkie usługi Acronis.
   a. Otwórz okno **Usługi**, a następnie wyłącz uruchamianie usług Acronis, z wyjątkiem usług **Acronis Active Protection Service** i **Acronis Cyber Protection Service**.



b. Otwórz narzędzie **Regedit**, a następnie wyłącz usługi **Acronis Active Protection Service** i **Acronis Cyber Protection Service**, edytując ich klucze:
   - W kluczu `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\AcronisCyberProtectionService` otwórz wartość **Start**, a następnie ustaw dane wartości na 4.
   - W kluczu `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\AcronisActiveProtectionService` otwórz wartość **Start**, a następnie ustaw dane wartości na 4.

2. Uruchom ponownie komputer serwera zarządzania, a następnie sprawdź, czy wyłączone usługi Acronis nie działają.

Uwaga
Dwie usługi — **Acronis Scheduler Service Helper** i **Acronis TIB Mounter Monitor** — nadal mogą działać. Można je spokojnie zignorować.

3. [Jeśli na komputerze serwera zarządzania jest zainstalowany komponent Cyber Protect Monitor] Zamknij komponent Acronis Cyber Protect Monitor.
4. W wierszu polecenia systemu Windows zmień właściciela folderów `%ProgramData%\Acronis` i `%ProgramFiles%\Acronis`, uruchamiając następujące polecenia:

```
takeown /f "%ProgramData%\Acronis" /r /d y
```

```
takeown /f "%ProgramFiles%\Acronis" /r /d y
```

5. Edytuj uprawnienia dostępu do tych folderów i ich podfolderów, uruchamiając następujące polecenia:

```
icacls "%ProgramData%\Acronis" /grant everyone:F /t
```

```
icacls "%ProgramFiles%\Acronis" /grant everyone:F /t
```

6. Skopiuj foldery `%ProgramData%\Acronis` i `%ProgramFiles%\Acronis` do udziału sieciowego, do którego nowy komputer serwer zarządzania ma dostęp.
7. Zamknij system pierwotnego komputera serwera zarządzania.

Następnie postępuj zgodnie z procedurą opisaną w sekcji "Operacje na komputerze docelowym" (s. 131).

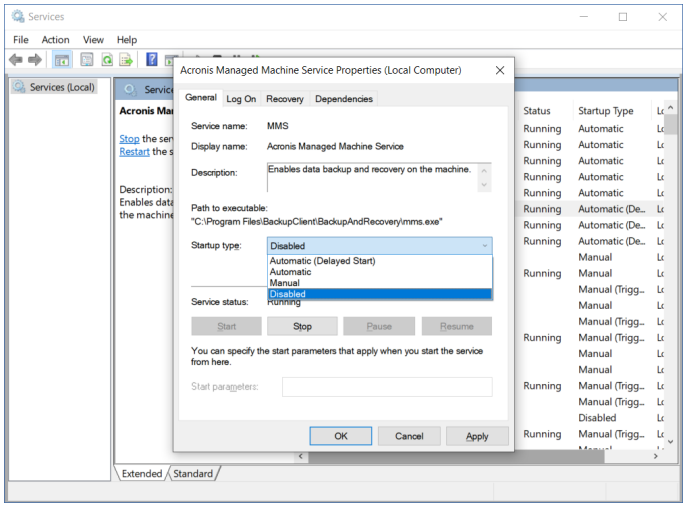
Operacje na komputerze docelowym

W tej fazie instaluje się i konfiguruje nowy serwer zarządzania, a następnie migruje na niego dane.

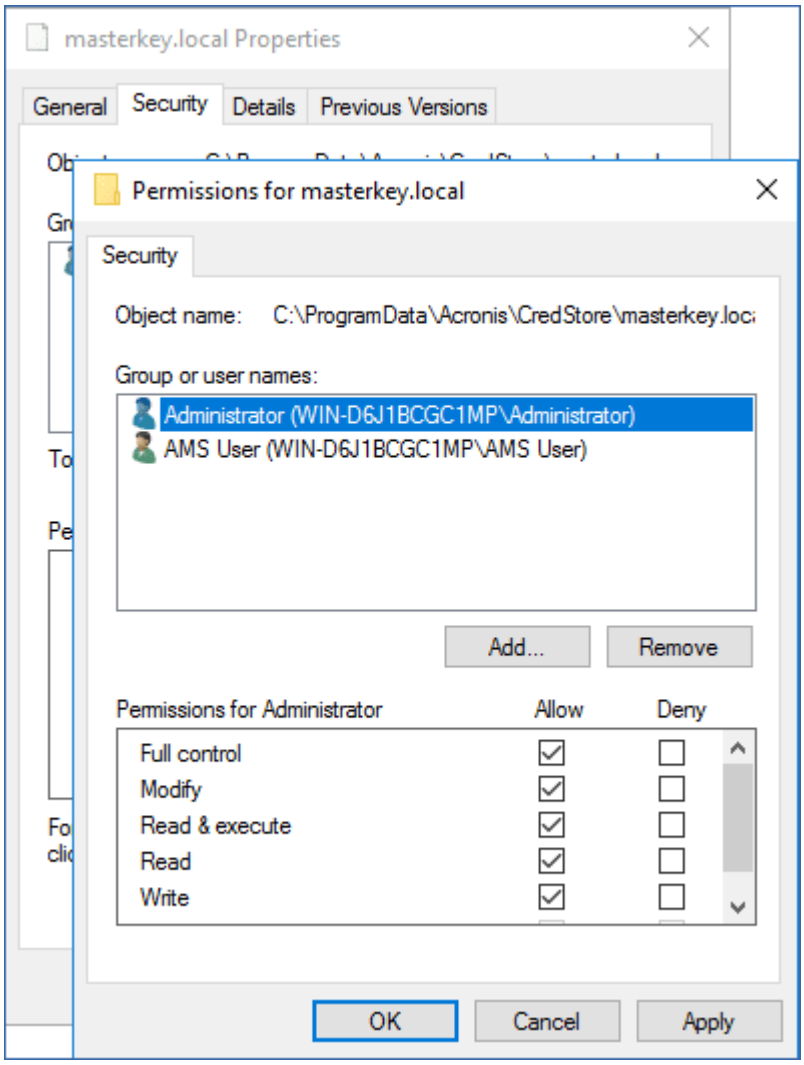
Zanim wykonasz operacje na komputerze docelowym, upewnij się, że została wykonana procedura opisana w sekcji "Operacje na komputerze źródłowym" (s. 130).

Aby migrować dane na nowy serwer zarządzania

1. Ustaw nazwę hosta komputera, na którym zostanie zainstalowany nowy serwer zarządzania. Nazwa ta musi być taka sama jak nazwa pierwotnego komputera serwera zarządzania.
2. Utwórz regułę zapory, aby zablokować cały ruch na porcie TCP 9877.
3. Uruchom program instalacyjny programu Acronis Cyber Protect.
   a. Zaakceptuj warunki umowy licencyjnej i zasady ochrony prywatności, a następnie kliknij **Kontynuuj**.
   b. Kliknij **Dostosuj ustawienia instalacji**.
   c. W polu **Elementy do zainstalowania** wybierz tylko poniższe komponenty, a następnie kliknij **Gotowe**.
      - Serwer zarządzania
      - Komponenty do instalacji zdalnej
      - Generator nośnika startowego
      - Narzędzie wiersza polecenia
   d. W polu **Baza danych na potrzeby serwera zarządzania** zachowaj opcję domyślną **Użyj wbudowanej bazy danych SQLite**.
   e. W polu **Konto logowania dla usługi serwera zarządzania** użyj tej samej opcji co na pierwotnym serwerze zarządzania.
4. Zatrzymaj wszystkie usługi Acronis.
   a. Otwórz okno **Usługi**, a następnie wyłącz uruchamianie wszystkich usług Acronis.



   b. Uruchom ponownie komputer, a następnie sprawdź, czy wyłączone usługi Acronis nie działają.
5. Przejdź do sekcji `%ProgramData%\Acronis\CredStore`, a następnie dostosuj uprawnienia do pliku `masterkey.local` następująco:
   a. Przyznaj własność pliku kontu użytkownika **Administrator**.
   b. Przyznaj kontu użytkownika **Administrator** uprawnienia **Pełna kontrola**.



6. Przejdź do folderu `%ProgramData%\Acronis\AMS\AccessVault\config`, a następnie przyznaj kontu użytkownika **Administrator** uprawnienia **Pełna kontrola** w odniesieniu do następujących plików:
   - `%ProgramData%\Acronis\AMS\AccessVault\config\preferred`
   - `%ProgramData%\Acronis\AMS\AccessVault\config\preferred.json`
7. Zastąp poniższe foldery folderami skopiowanymi do udziału sieciowego z pierwotnego komputera serwera zarządzania:
   - `%ProgramData%\Acronis`
   - `%ProgramFiles%\Acronis`

Ważne
Zastąp istniejące foldery bez uprzedniego ich usuwania.

Uwaga
Jeśli pojawi się komunikat, że nie można zastąpić folderu `%ProgramFiles%\Acronis\ShellExtentions`, możesz spokojnie pominąć ten folder.

8. Przywróć uprawnienia w przypadku następujących plików:
   - `%ProgramData%\Acronis\CredStore\masterkey.local` — usuń konto użytkownika **Administrator** z listy użytkowników z uprawnieniami.
   - `%ProgramData%\Acronis\AMS\AccessVault\config\preferred` — przyznaj kontu użytkownika **Administrator** tylko uprawnienie **Odczyt**.
   - `%ProgramData%\Acronis\AMS\AccessVault\config\preferred.json` — przyznaj kontu użytkownika **Administrator** tylko uprawnienie **Odczyt**.
9. Utwórz połączenie katalogów dla folderu `NGMP\latest`.
   - W wierszu polecenia systemu Windows przejdź do folderu `%ProgramData%\Acronis\NGMP`, a następnie usuń folder `latest`.

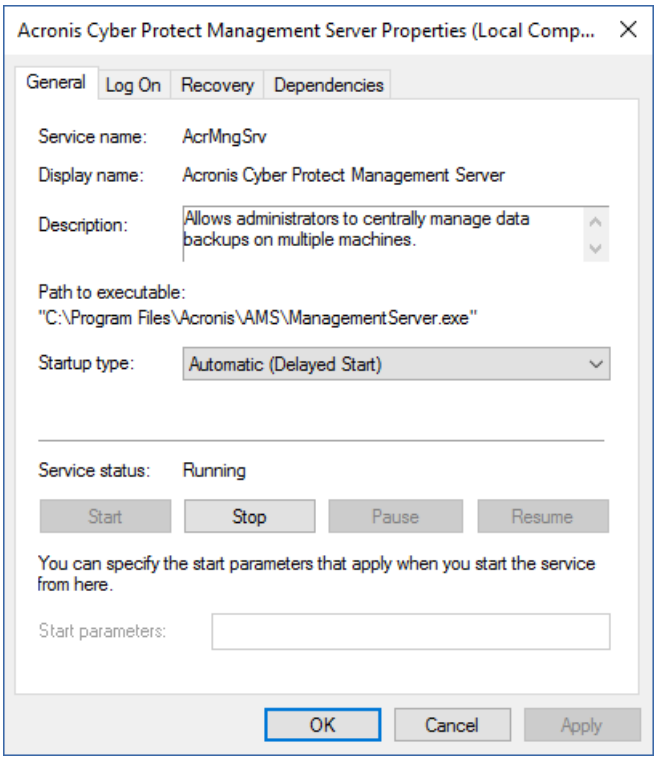
     ```
     cd %ProgramData%\Acronis\NGMP
     ```

     ```
     rmdir latest
     ```

   - Utwórz połączenie katalogów dla folderu `latest` i wskaż go w folderze o nazwie zgodnej z bieżącą wersją NGMP, na przykład:

     ```
     mklink /j latest C:\ProgramData\Acronis\NGMP\1.0.2653.0
     ```

10. Na nowym serwerze zarządzania wskaż bazę danych Microsoft SQL Server, z której korzystał pierwotny serwer zarządzania.
    a. Otwórz narzędzie **Regedit**.
    b. W kluczu `HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\AMS\Settings` zmień dane wartości `AmsDmlDbProtocol` na `config://C:\ProgramData\Acronis\AMS\mssql\dml_mssql.config`.
11. Otwórz okno **Usługi**, a następnie włącz wszystkie wyłączone usługi Acronis.
    Ustaw typ uruchamiania usługi **Acronis Cyber Protect Management Server** na **Automatycznie (opóźnione uruchomienie)**, a typ uruchamiania pozostałych usług Acronis na **Automatycznie**.



12. W zaporze zezwól na cały ruch na porcie TCP 9877.
13. Uruchom ponownie komputer, a następnie sprawdź, czy działają wszystkie usługi Acronis.
14. Uruchom program instalacyjny Acronis Cyber Protect i zainstaluj następujące elementy:
    - Agent dla systemu Windows
    - [Opcjonalnie] Cyber Protect Monitor
15. Uruchom ponownie komputer.

Wdrożenie chmurowe

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 internetowej Cyber Protect.** Za pomocą tego łącza możesz uzyskiwać dostęp do konsoli w przyszłości. Nazwa logowania i hasło są takie same jak te, które zostały użyte w poprzednim kroku.

Przygotowanie

Krok 1

Wybierz agenta w zależności od elementów, których kopię zapasową chcesz utworzyć. Informacje na temat agentów można znaleźć w sekcji "Komponenty" (s. 48).

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 opisano tutaj: "Wdrażanie agentów przy użyciu zasad grupy" (s. 182).

Aby pobrać program instalacyjny agenta dla usługi Office 365, kliknij ikonę konta w prawym górnym rogu, a następnie kliknij **Do pobrania** > **Agent dla usługi Office 365**.

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

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

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:

- Porty **443** i **8443**

  Porty te służą do uzyskiwania dostępu do konsoli internetowej Cyber Protect, rejestrowania agentów, pobierania certyfikatów, autoryzacji użytkowników oraz pobierania plików z chmury.
- Porty w zakresie **7770**–**7800**

  Agenty używają tych portów do komunikacji z serwerem zarządzania.
- Porty **44445** i **55556**

  Agenty używają tych portów do przesyłania danych podczas tworzenia kopii zapasowych i odzyskiwania.

Jeśli w danej sieci jest włączony serwer proxy, zajrzyj do sekcji „"Ustawienia serwera proxy" (s. 138)”, aby sprawdzić, czy trzeba skonfigurować te ustawienia na każdym komputerze, na którym działa agent ochrony.

Minimalna prędkość łącza internetowego niezbędna do zarządzania agentem z chmury to 1 Mb/s (nie mylić z minimalną prędkością transmisji danych do tworzenia kopii zapasowych w chmurze). Należy o tym pamiętać w przypadku korzystania z połączeń o niskiej przepustowości, na przykład ADSL.

Porty TCP wymagane do operacji tworzenia kopii zapasowych i replikacji maszyn wirtualnych VMware

- Port **443**

  Agent dla VMware (zarówno Windows, jak i urządzenie wirtualne) łączy się z tym portem hosta ESXi lub serwera vCenter w celu wykonania operacji zarządzania maszynami wirtualnymi, takich jak utworzenie, aktualizacja i usunięcie maszyn wirtualnych w vSphere podczas operacji tworzenia kopii zapasowych, odzyskiwania oraz replikacji maszyn wirtualnych.
- Port **902**

  Agent dla VMware (zarówno Windows, jak i urządzenie wirtualne) łączy się z tym portem hosta ESXi w celu ustanowienia połączenia NFC na potrzeby odczytu/zapisu danych na maszynach wirtualnych podczas operacji tworzenia kopii zapasowych, odzyskiwania i replikacji maszyn wirtualnych.
- Port **3333**

  Jeśli agent dla VMware (urządzenie wirtualne) działa na hoście/klastrze ESXi, który jest obiektem docelowym replikacji maszyny wirtualnej, ruch związany z replikacją maszyny wirtualnej nie trafia bezpośrednio do hosta ESXi na port **902**. Zamiast tego ruch trafia od źródłowego agenta dla VMware na port TCP **3333** agenta dla VMware (urządzenie wirtualne) znajdującego się na docelowym hoście/klastrze ESXi.

  Źródłowy agent dla VMware, który odczytuje dane z oryginalnych dysków VMware, może się znajdować w dowolnym miejscu i być dowolnego typu: urządzenie wirtualne lub Windows.

  Usługa, która odpowiada za przyjmowanie danych replikacji maszyny wirtualnej w docelowym agencie dla VMware (urządzenie wirtualne), nosi nazwę „Serwer dysków replik”. Usługa ta odpowiada za techniki optymalizacji sieci WAN, takie jak kompresja ruchu i deduplikacja podczas replikacji maszyn wirtualnych, w tym seeding replik (zobacz Seeding repliki początkowej).W sytuacji, gdy na docelowym hoście ESXi nie działa agent dla VMware (urządzenie wirtualne), usługa ta nie jest dostępna, w związku z czym scenariusz seedingu replik nie jest obsługiwany.

Krok 4

Sprawdź, czy na komputerze, na którym planujesz zainstalować agenta ochrony, inne procesy nie używają poniższych portów lokalnych.

- 127.0.0.1:**9999**
- 127.0.0.1:**43234**

- 127.0.0.1:**9850**

Uwaga
Nie trzeba ich otwierać na zaporze.

Usługa Active Protection nasłuchuje na porcie TCP **6109**. Upewnij się, że nie jest on używany przez inny proces.

Zmienianie portów używanych przez agenta ochrony

Niektóre porty wymagane przez agenta ochrony mogą być używane przez inne aplikacje w środowisku. Aby uniknąć konfliktów, można zmienić domyślne porty używane przez agenta ochrony, modyfikując następujące pliki.

- W systemie Linux: `/opt/Acronis/etc/aakore.yaml`
- W systemie Windows: `\ProgramData\Acronis\Agent\etc\aakore.yaml`

Ustawienia serwera proxy

Agenty ochrony mogą przesyłać dane przez serwer proxy HTTP/HTTPS. Serwer musi działać przez tunel HTTP bez skanowania ruchu HTTP lub ingerowania w niego. Serwery proxy działające w trybie MITM (man-in-the-middle) nie są obsługiwane.

Ponieważ agent podczas instalacji rejestruje się w chmurze, ustawienia serwera proxy muszą zostać podane podczas instalacji lub wcześniej.

W systemie Windows

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. Ustawienia serwera proxy można wprowadzić podczas instalacji lub z wyprzedzeniem, korzystając z niżej opisanej procedury. Aby zmienić ustawienia serwera proxy po instalacji, należy skorzystać z tej samej procedury.

Aby określić ustawienia serwera proxy 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
"Login"="proxy_login"
"Password"="proxy_password"
```

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. Jeśli serwer proxy wymaga uwierzytelnienia, zastąp `proxy_login` i `proxy_hasło` poświadczeniami serwera proxy. W przeciwnym razie usuń te wiersze z pliku.
5. Zapisz dokument pod nazwą **proxy.reg**.
6. Uruchom plik jako administrator.
7. Potwierdź, że chcesz edytować rejestr systemu Windows.
8. Jeśli agent ochrony 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
```

W systemie Linux

Uruchom plik instalacyjny z następującymi parametrami: `--http-proxy-host=ADRES --http-proxy-port=PORT --http-proxy-login=NAZWA_LOGOWANIA--http-proxy-password=HASŁO`. Aby zmienić ustawienia serwera proxy po instalacji, należy skorzystać z niżej opisanej procedury.

Aby zmienić ustawienia serwera proxy w systemie Linux

1. Otwórz plik **/etc/Acronis/Global.config** w edytorze tekstowym.
2. Wykonaj jedną z następujących czynności:
   - Jeśli ustawienia serwera proxy zostały określone podczas instalacji agenta, znajdź następującą sekcję:

```
<key name="HttpProxy">
    <value name="Enabled" type="Tdword">"1"</value>
    <value name="Host" type="TString">"ADDRESS"</value>
    <value name="Port" type="Tdword">"PORT"</value>
    <value name="Login" type="TString">"LOGIN"</value>
    <value name="Password" type="TString">"PASSWORD"</value>
</key>
```

   - W przeciwnym wypadku skopiuj powyższe wiersze i wklej je do pliku między znacznikami `<registry name="Global">...</registry>`.
3. Zastąp wartość `ADRES` nową nazwą hosta / adresem IP serwera proxy, a wartość `PORT` — wartością dziesiętną numeru portu.
4. Jeśli serwer proxy wymaga uwierzytelnienia, zastąp `NAZWA LOGOWANIA` i `HASŁO` poświadczeniami serwera proxy. W przeciwnym razie usuń te wiersze z pliku.
5. Zapisz plik.

6. W przeciwnym wypadku uruchom ponownie agenta, wykonując w dowolnym katalogu następujące polecenie:

```
sudo service acronis_mms restart
```

W systemie macOS

Ustawienia serwera proxy można wprowadzić podczas instalacji lub z wyprzedzeniem, korzystając z niżej opisanej procedury. Aby zmienić ustawienia serwera proxy po instalacji, należy skorzystać z tej samej procedury.

Aby określić ustawienia serwera proxy w systemie macOS

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

```
<?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>
    <value name="Login" type="TString">"nazwa_logowania_proxy"</value>
    <value name="Password" type="TString">"hasło_serwera_proxy"</value>
  </key>
</registry>
```

3. Zastąp `proxy.company.com` nazwą hosta / adresem IP serwera proxy, a `443` — wartością dziesiętną numeru portu.
4. Jeśli serwer proxy wymaga uwierzytelnienia, zastąp `proxy_login` i `proxy_hasło` poświadczeniami serwera proxy. W przeciwnym razie usuń te wiersze z pliku.
5. Zapisz plik.
6. Jeśli agent ochrony 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
```

Na nośniku startowym

Podczas pracy z nośnikiem startowym może wystąpić konieczność uzyskania dostępu do chmury za pośrednictwem serwera proxy. Aby określić ustawienia serwera proxy, kliknij **Narzędzia** > **Serwer proxy**, a następnie podaj nazwę hosta / adres IP, port i poświadczenia serwera proxy.

Instalowanie agentów

W systemie Windows

1. Upewnij się, że komputer ma połączenie z Internetem.
2. Zaloguj się jako administrator i uruchom program instalacyjny.
3. [Opcjonalnie] Kliknij **Dostosuj ustawienia instalacji** i wprowadź odpowiednie zmiany, jeśli chcesz:
   - Zmienić komponenty do zainstalowania (przede wszystkim wyłączyć instalację komponentów Cyber Protect Monitor i Narzędzia wiersza polecenia).
   - Zmienić metodę rejestracji komputera w usłudze Cyber Protection. Możesz przełączyć z opcji **Użyj konsoli Cyber Protect** (opcja domyślna) na opcję **Użyj poświadczeń** lub **Użyj tokenu rejestracji**.
   - Zmienić ścieżkę instalacji.
   - Zmienić konto usługi agenta.
   - Aby zweryfikować lub zmienić nazwę hosta / adres IP, port i poświadczenia serwera proxy. W przypadku włączenia serwera proxy w systemie Windows zostanie on automatycznie wykryty i użyty.
4. Kliknij **Zainstaluj**.
5. [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, a następnie kliknij **Gotowe**. Zalecamy korzystanie z konta, które ma przypisaną rolę **Administrator**. W innym przypadku należy zadbać o dostęp do konta mającego niezbędne uprawnienia na serwerze vCenter lub ESXi.
6. [Tylko w przypadku instalowania na kontrolerze domeny] Określ konto użytkownika, które będzie służyć do uruchamiania usługi agenta, a następnie kliknij **Gotowe**. Ze względów bezpieczeństwa program instalacyjny nie tworzy automatycznie nowych kont na kontrolerze domeny.

   Uwaga
   Wskazane konto użytkownika musi mieć przyznane prawo `Logowanie jako usługa`.
   Konto to musi już być używane na kontrolerze domeny, aby jego folder profilu został utworzony na tym komputerze.

   Dodatkowe informacje o instalowaniu agenta na kontrolerze domeny w trybie tylko do odczytu można znaleźć w tym artykule z bazy wiedzy Knowledge Base.
7. Jeśli w kroku 3 została zachowana domyślna metoda rejestracji **Użyj konsoli Cyber Protect**, poczekaj, aż pojawi się ekran rejestracji, a następnie przejdź do następnego kroku. W przeciwnym razie nie trzeba wykonywać żadnych innych czynności.

8. Wykonaj jedną z następujących czynności:
   - Kliknij **Zarejestruj komputer**. W otwartym oknie przeglądarki zaloguj się do konsoli internetowej Cyber Protect, przejrzyj dane rejestracji i kliknij **Potwierdź rejestrację**.
   - Kliknij **Pokaż informacje rejestracyjne**. W programie instalacyjnym zostaną wyświetlone łącze oraz kod rejestracji. Możesz je skopiować i dokonać rejestracji na innym komputerze. W takim przypadku będzie konieczne wprowadzenie kodu rejestracji w formularzu rejestracyjnym. Kod rejestracji jest ważny przez godzinę.

     Aby otworzyć formularz rejestracyjny, możesz też kliknąć **Wszystkie urządzenia** > **Dodaj**, przewinąć w dół do pozycji **Rejestracja przy użyciu kodu**, a następnie kliknąć **Zarejestruj**.
9. **Uwaga**
   Nie zamykaj programu instalacyjnego, dopóki nie potwierdzisz rejestracji. Aby ponownie zainicjować rejestrację, trzeba ponownie uruchomić program instalacyjny, a następnie kliknąć **Zarejestruj komputer**.

   W wyniku tych działań komputer zostanie przypisany do konta użytego do zalogowania się do konsoli internetowej Cyber Protect.

W systemie Linux

1. Upewnij się, że komputer ma połączenie z Internetem.
2. Uruchom plik instalacyjny jako użytkownik root.

   Jeśli w sieci jest włączony serwer proxy, podczas uruchamiania pliku należy podać nazwę hosta / adres IP oraz port tego serwera w następującym formacie: `--http-proxy-host=ADRES --http-proxy-port=PORT --http-proxy-login=NAZWA LOGOWANIA--http-proxy-password=HASŁO`.

   Jeśli chcesz zmienić domyślną metodę rejestracji komputera w usłudze Cyber Protection, uruchom plik instalacyjny przy użyciu jednego z poniższych parametrów:
   - `--register-with-credentials` — powoduje wyświetlenie monitu o nazwę użytkownika i hasło podczas instalacji.
   - `--token=CIĄG` — umożliwia wymuszenie użycia tokenu rejestracji.
   - `--skip-registration` — umożliwia pominięcie rejestracji.
3. 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.
4. W przypadku zachowania w kroku 2 domyślnej metody rejestracji, przejdź do następnego kroku. W przeciwnym razie wprowadź nazwę użytkownika i hasło do usługi Cyber Protection lub poczekaj, aż komputer zostanie zarejestrowany za pomocą tokenu.

5. Wykonaj jedną z następujących czynności:
   - Kliknij **Zarejestruj komputer**. W otwartym oknie przeglądarki zaloguj się do konsoli internetowej Cyber Protect, przejrzyj dane rejestracji i kliknij **Potwierdź rejestrację**.
   - Kliknij **Pokaż informacje rejestracyjne**. W programie instalacyjnym zostaną wyświetlone łącze oraz kod rejestracji. Możesz je skopiować i dokonać rejestracji na innym komputerze. W takim przypadku będzie konieczne wprowadzenie kodu rejestracji w formularzu rejestracyjnym. Kod rejestracji jest ważny przez godzinę.

     Aby otworzyć formularz rejestracyjny, możesz też kliknąć **Wszystkie urządzenia** > **Dodaj**, przewinąć w dół do pozycji **Rejestracja przy użyciu kodu**, a następnie kliknąć **Zarejestruj**.

6. **Uwaga**
   Nie zamykaj programu instalacyjnego, dopóki nie potwierdzisz rejestracji. Aby ponownie zainicjować rejestrację, trzeba będzie ponownie uruchomić program instalacyjny i jeszcze raz wykonać procedurę instalacji.

   W wyniku tych działań komputer zostanie przypisany do konta użytego do zalogowania się do konsoli internetowej Cyber Protect.
7. Jeśli na komputerze jest włączona funkcja UEFI Secure Boot, pojawi się informacja o konieczności ponownego uruchomienia systemu po zakończeniu instalacji. Koniecznie zapamiętaj, jakiego hasła (hasła użytkownika root czy hasła „acronis”) należy użyć.

   Uwaga
   W trakcie instalacji zostanie wygenerowany nowy klucz, który posłuży do podpisania modułu `snapapi`. Zostanie on zarejestrowany jako Klucz właściciela komputera. W celu zarejestrowania tego klucza konieczne jest ponowne uruchomienie. Bez rejestracji klucza agent nie będzie działać. Jeśli funkcja UEFI Secure Boot zostanie włączona po instalacji agenta, powtórz instalację, w tym krok 6.

8. Po instalacji wykonaj jedną z następujących czynności:
   - Jeśli w ramach poprzedniego kroku pojawił się monit o ponowne uruchomienie systemu, kliknij **Uruchom ponownie**.

     Podczas ponownego uruchamiania systemu wybierz opcję zarządzania kluczem właściciela komputera, zaznacz **Zarejestruj klucz właściciela komputera**, a następnie zarejestruj klucz przy użyciu hasła zalecanego w poprzednim kroku.
   - W przeciwnym razie kliknij **Zakończ**.

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

W systemie macOS

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 w danej sieci jest włączony serwer proxy, kliknij **Agent ochrony** na pasku menu, kliknij **Ustawienia serwera proxy**, a następnie podaj nazwę hosta lub adres IP serwera proxy, jego port oraz odpowiednie poświadczenia dostępu.
6. Jeśli pojawi się monit, podaj poświadczenia administratora.
7. Kliknij **Kontynuuj**.
8. Poczekaj, aż pojawi się ekran rejestracji.
9. Wykonaj jedną z następujących czynności:
   - Kliknij **Zarejestruj komputer**. W otwartym oknie przeglądarki zaloguj się do konsoli internetowej Cyber Protect, przejrzyj dane rejestracji i kliknij **Potwierdź rejestrację**.
   - Kliknij **Pokaż informacje rejestracyjne**. W programie instalacyjnym zostaną wyświetlone łącze oraz kod rejestracji. Możesz je skopiować i dokonać rejestracji na innym komputerze. W takim przypadku będzie konieczne wprowadzenie kodu rejestracji w formularzu rejestracyjnym. Kod rejestracji jest ważny przez godzinę.
     Aby otworzyć formularz rejestracyjny, możesz też kliknąć **Wszystkie urządzenia** > **Dodaj**, przewinąć w dół do pozycji **Rejestracja przy użyciu kodu**, a następnie kliknąć **Zarejestruj**.
10. **Wskazówka** Nie zamykaj programu instalacyjnego, dopóki nie potwierdzisz rejestracji. Aby ponownie zainicjować rejestrację, trzeba będzie ponownie uruchomić program instalacyjny i jeszcze raz wykonać procedurę instalacji.

W wyniku tych działań komputer zostanie przypisany do konta użytego do zalogowania się do konsoli internetowej Cyber Protect.

Zmienianie konta logowania na komputerach z systemem Windows

Na ekranie **Wybierz komponenty** wskaż konto, na którym będą działać usługi, w polu **Konto logowania dla usługi agenta**. Można wybrać jedną z następujących opcji:

- **Użyj kont użytkowników usługi** (domyślne w przypadku usługi agenta)
  Konta użytkowników usługi to konta w systemie Windows używane do uruchamiania usług. Ustawienie to ma tę zaletę, że zasady zabezpieczeń domeny nie wpływają na prawa użytkowników tych kont. Domyślnie agent działa na koncie **System lokalny**.
- **Utwórz nowe konto**
  Nazwą konta dla danego agenta będzie Agent User.
- **Użyj następującego konta**
  Jeśli agent zostanie zainstalowany na kontrolerze domeny, system wyświetli monit o określenie istniejących już kont (lub tego samego konta) na potrzeby agenta. Ze względów bezpieczeństwa system nie tworzy automatycznie nowych kont na kontrolerze domeny.
  Konto użytkownika określone podczas uruchamiania programu instalacyjnego na kontrolerze domeny musi mieć przyznane prawo `Logowanie jako usługa`. Konto to musi już być używane na kontrolerze domeny, aby jego folder profilu został utworzony na tym komputerze.

Dodatkowe informacje o instalowaniu agenta na kontrolerze domeny w trybie tylko do odczytu można znaleźć w tym artykule z bazy wiedzy Knowledge Base.

W przypadku wybrania opcji **Utwórz nowe konto** lub **Użyj następującego konta** dopilnuj, aby zasady zabezpieczeń domeny nie wpływały na prawa powiązanych kont. Jeśli konto straci prawa użytkownika przypisane podczas instalacji, komponent może działać niepoprawnie lub wcale nie działać.

Uprawnienia wymagane w przypadku konta logowania

Agent ochrony jest uruchamiany jako usługa Managed Machine Service (MMS) na komputerze z systemem Windows. Aby agent działał jak należy, konto, na którym zostanie uruchomiony, musi mieć określone prawa. Dlatego też użytkownikowi usługi MMS należy przyznać następujące uprawnienia:

1. Przynależność do grup **Operatorzy kopii zapasowych** i **Administratorzy**. W przypadku kontrolera domeny użytkownik musi należeć do grupy **Administratorzy domeny**.
2. Uprawnienie **Pełna kontrola** do folderu `%PROGRAMDATA%\Acronis` (w systemach Windows XP i Server 2003, `%ALLUSERSPROFILE%\Application Data\Acronis`) i do podfolderów.
3. Uprawnienie **Pełna kontrola** do pewnych kluczy rejestru w kluczu: `HKEY_LOCAL_MACHINE\SOFTWARE\Acronis`.
4. Przyznane następujące prawa użytkownika:
   - Zaloguj jako usługa
   - Dostosuj przydziały pamięci dla procesu
   - Zamień token na poziomie procesu
   - Modyfikuj wartości środowiskowe oprogramowania układowego

Jak przypisać prawa użytkownika

Aby przypisać prawa użytkownika, należy postąpić zgodnie z poniższymi instrukcjami (w przykładzie posłużono się prawem użytkownika **Logowanie w trybie usługi**, ale instrukcje są takie same w przypadku wszystkich praw):

1. Zaloguj się do komputera przy użyciu konta z uprawnieniami administracyjnymi.
2. Otwórz **Narzędzia administracyjne** w **Panelu sterowania** (lub naciśnij Win+R, wpisz **control admintools** i naciśnij Enter) i otwórz **Zasady zabezpieczeń lokalnych**.
3. Rozwiń gałąź **Zasady lokalne** i kliknij **Przypisywanie praw użytkownika**.
4. W prawym okienku kliknij prawym przyciskiem myszy **Logowanie w trybie usługi** i wybierz **Właściwości**.
5. Kliknij przycisk **Dodaj użytkownika lub grupę**, aby dodać nowego użytkownika.
6. W oknie **Wybierz użytkowników, komputery, konta usług lub grupy** znajdź właściwego użytkownika i kliknij **OK**.
7. Kliknij **OK** w obszarze **Logowanie w trybie usługi — właściwości**, aby zapisać zmiany.

Ważne
Dopilnuj, aby użytkownik, któremu przyznano prawo **Logowanie w trybie usługi**, nie znajdował się na liście zasad **Odmowa logowania w trybie usługi** w sekcji **Zasady zabezpieczeń lokalnych**.

Uwaga: ręczna zmian kont logowania po zakończeniu instalacji nie jest zalecana.

Instalacja nienadzorowana lub dezinstalacja

Instalacja nienadzorowana lub dezinstalacja w systemie Windows

W tej sekcji opisano, jak zainstalować lub odinstalować agenty ochrony w trybie nienadzorowanym na komputerze z systemem Windows za pomocą Instalatora Windows (programu `msiexec`). W domenie Active Directory instalację nienadzorowaną można wykonać również przy użyciu zasad grupy — zobacz "Wdrażanie agentów przy użyciu zasad grupy" (s. 182).

Podczas instalacji można skorzystać z tzw. **pliku transformacji** (pliku .mst). Plik transformacji zawiera parametry instalacji. Parametry instalacji można też podać bezpośrednio w wierszu polecenia.

Tworzenie transformacji .mst i wyodrębnianie pakietów instalacyjnych

1. Zaloguj się jako administrator i uruchom program instalacyjny.
2. Kliknij **Utwórz pliki .mst i .msi na potrzeby instalacji nienadzorowanej**.
3. W polu **Elementy do zainstalowania** wybierz komponenty, które chcesz zainstalować, a następnie kliknij **Gotowe**.
   Z programu instalacyjnego zostaną wyodrębnione pakiety instalacyjne tych komponentów.
4. W polu **Ustawienia rejestracji** wybierz **Użyj poświadczeń** lub **Użyj tokenu rejestracji**.
   Dodatkowe informacje o procedurze generowania tokenu rejestracji można znaleźć w sekcji "Krok 1: Generowanie tokenu rejestracji" (s. 183).
5. [Tylko w przypadku instalowania na kontrolerze domeny] W obszarze **Konto logowania dla usługi agenta** wybierz **Użyj następującego konta**. Określ konto użytkownika, które będzie służyć do uruchamiania usługi agenta, a następnie kliknij **Gotowe**. Ze względów bezpieczeństwa program instalacyjny nie tworzy automatycznie nowych kont na kontrolerze domeny.

   Uwaga
   Wskazane konto użytkownika musi mieć przyznane prawo `Logowanie jako usługa`.
   Konto to musi już być używane na kontrolerze domeny, aby jego folder profilu został utworzony na tym komputerze.

   Dodatkowe informacje o instalowaniu agenta na kontrolerze domeny w trybie tylko do odczytu można znaleźć w tym artykule z bazy wiedzy Knowledge Base.
6. Przejrzyj lub zmodyfikuj inne ustawienia instalacji, które zostaną dodane do pliku .mst, a następnie kliknij **Kontynuuj**.

7. Wybierz folder, w którym zostanie wygenerowana transformacja .mst i zostaną wyodrębnione pakiety instalacyjne .msi i .cab, a następnie kliknij **Wygeneruj**.

Instalowanie programu przy użyciu pliku transformacji .mst

W wierszu polecenia uruchom następujące polecenie.

Wzór polecenia:

```
msiexec /i <package name> TRANSFORMS=<transform name>
```

Gdzie:

- `<nazwa pakietu>` oznacza nazwę pliku .msi.
- `<nazwa przekształcenia>` oznacza nazwę transformacji.

Przykład polecenia:

```
msiexec /i BackupClient64.msi TRANSFORMS=BackupClient64.msi.mst
```

Instalowanie lub odinstalowywanie programu przez ręczne określenie parametrów

W wierszu polecenia uruchom następujące polecenie.

Wzór polecenia (instalacja):

```
msiexec /i <package name><PARAMETER 1>=<value 1> ... <PARAMETER N>=<value n>
```

`<nazwa pakietu>` oznacza tu nazwę pliku .msi. Wszystkie dostępne parametry i ich wartości opisano w sekcji "Podstawowe parametry" (s. 147).

Wzór polecenia (dezinstalacja):

```
msiexec /x <package name> <PARAMETER 1>=<value 1> ... <PARAMETER N>=<value n>
```

Pakiet .msi musi być w tej samej wersji co odinstalowywany produkt.

Parametry instalacji nienadzorowanej lub dezinstalacji

W tej sekcji opisano parametry używane podczas instalacji nienadzorowanej lub dezinstalacji w systemie Windows. Oprócz tych parametrów można tez używać innych parametrów programu `msiexec` zgodnie z opisem podanym w artykule https://msdn.microsoft.com/en-us/library/windows/desktop/aa367988(v=vs.85).aspx.

Parametry instalacji

Podstawowe parametry

`ADDLOCAL=<list of components>`

Nazwy komponentów do zainstalowania, rozdzielone przecinkami bez spacji. Przed instalacją należy wyodrębnić z programu instalacyjnego wszystkie wskazane komponenty.

Oto pełna lista komponentów:

Komponent	Inne wymagane równolegle komponenty	Bitowość	Nazwa/opis komponentu
MmsMspComponents		wersja 32-bitowa/64-bitowa	Podstawowe komponenty dla agentów
BackupAndRecoveryAgent	MmsMspComponents	wersja 32-bitowa/64-bitowa	Agent dla systemu Windows
ArxAgentFeature	BackupAndRecoveryAgent	wersja 32-bitowa/64-bitowa	Agent dla programu Exchange
ArsAgentFeature	BackupAndRecoveryAgent	wersja 32-bitowa/64-bitowa	Agent dla SQL
ARADAgentFeature	BackupAndRecoveryAgent	wersja 32-bitowa/64-bitowa	Agent dla usługi Active Directory
ArxOnlineAgentFeature	MmsMspComponents	wersja 32-bitowa/64-bitowa	Agent dla usługi Office 365
OracleAgentFeature	BackupAndRecoveryAgent	wersja 32-bitowa/64-bitowa	Agent dla programu Oracle
AcronisESXSupport	MmsMspComponents	64-bitowy	Agent dla VMware ESX(i) (Windows)
HyperVAgent	MmsMspComponents	wersja 32-bitowa/64-bitowa	Agent dla Hyper-V
CommandLineTool		wersja 32-bitowa/64-bitowa	Narzędzie wiersza polecenia
TrayMonitor	BackupAndRecoveryAgent	wersja 32-	Cyber Protect

		bitowa/64-bitowa	Monitor

`TARGETDIR= <path>`

Folder, w którym chcesz zainstalować program. Domyślnie jest to folder: `C:\Program Files\BackupClient`.

`REBOOT=ReallySuppress`

W przypadku określenia tego parametru ponowny rozruch komputera jest wzbroniony.

`/l*v <log file>`

W przypadku określenia tego parametru we wskazanym pliku zostanie zapisany dziennik instalacji w trybie informacji pełnej. Pliku dziennika można użyć do analizowania problemów z instalacją.

`CURRENT_LANGUAGE= <language ID>`

Język programu. Dostępne są następujące wartości: `en, bg, cs, da, de, es, fr, hu, id, it, ja, ko, ms, nb, nl, pl, pt, pt_BR, ru, fi, sr, sv, tr, zh, zh_TW`.
Jeśli ten parametr nie zostanie określony, język produktu zostanie zdefiniowany na podstawie języka systemu, pod warunkiem, że znajduje się on na powyższej liście. Jeśli go nie ma, język produktu zostanie ustawiony na język angielski (`en`).

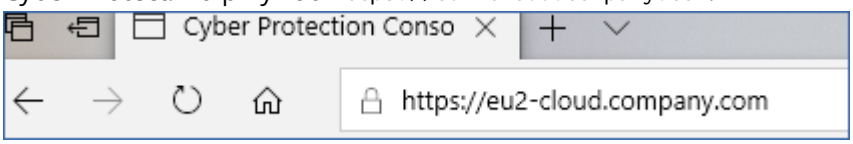
Parametry rejestracji

`REGISTRATION_ADDRESS`

To jest adres URL usługi Cyber Protect. Tego parametru można użyć albo z parametrami `REGISTRATION_LOGIN` i `REGISTRATION_PASSWORD` , albo z parametrem `REGISTRATION_TOKEN`.

- W przypadku użycia parametru `REGISTRATION_ADDRESS` z parametrami `REGISTRATION_LOGIN` i `REGISTRATION_PASSWORD` należy podać adres używany **do logowania się** do usługi Cyber Protect. Na przykład `https://cloud.company.com`:

- W przypadku użycia parametru `REGISTRATION_ADDRESS` z parametrem `REGISTRATION_TOKEN` należy podać dokładny adres centrum danych. Jest to adres URL widoczny **po zalogowaniu się** do usługi Cyber Protect. Na przykład `https://eu2-cloud.company.com`.



  W tym przypadku nie używaj `https://cloud.company.com`.

`REGISTRATION_LOGIN` i `REGISTRATION_PASSWORD`

Poświadczenia dostępu do konta, na którym zostanie zarejestrowany agent w usłudze Cyber Protect. Nie może to być konto administratora partnera.

`REGISTRATION_PASSWORD_ENCODED`

Hasło do konta, na którym zostanie zarejestrowany agent w usłudze Cyber Protect, zakodowane w formacie base64. Więcej informacji o procedurze kodowania hasła można znaleźć w sekcji „Ręczne rejestrowanie komputerów”.

`REGISTRATION_TOKEN`

Token rejestracji to ciąg 12 znaków podzielony dywizami na trzy części. Można go wygenerować w konsoli internetowej <PRODUCT_NAME> zgodnie z instrukcją podaną w sekcji „Wdrażanie agentów przy użyciu zasad grupy”.

`REGISTRATION_REQUIRED={0,1}`

Umożliwia określenie sposobu ukończenia instalacji w razie niepowodzenia rejestracji. W przypadku wartości `1` instalacja również się nie powiedzie. Wartością domyślną jest `0`, więc jeśli nie określisz tego parametru, instalacja przebiegnie pomyślnie, mimo że agent nie został zarejestrowany.

Dodatkowe parametry

Aby zdefiniować konto logowania dla usługi agenta w systemie Windows, należy użyć jednego z poniższych parametrów:

- `MMS_USE_SYSTEM_ACCOUNT={0,1}`

  W przypadku wartości `1` agent będzie działać na koncie **System lokalny**.
- `MMS_CREATE_NEW_ACCOUNT={0,1}`

  W przypadku wartości `1` agent będzie działać na nowo utworzonym koncie o nazwie **Acronis Agent User**.
- `MMS_SERVICE_USERNAME=<user name>` i `MMS_SERVICE_PASSWORD=<password>`

  Użyj tych parametrów, aby wskazać już istniejące konto, na którym będzie działać agent.

Więcej informacji na temat kont logowania można znaleźć w sekcji „Zmienianie konta logowania na komputerach z systemem Windows”.

`SET_ESX_SERVER={0,1}`

- W przypadku wartości `0` nie będzie ustanawiane połączenie między instalowanym agentem dla VMware a serwerem vCenter lub hostem ESXi. W przypadku wartości `1` określ następujące parametry:
  - `ESX_HOST=<host name>`

    Nazwa hosta lub adres IP serwera vCenter lub hosta ESXi.
  - `ESX_USER=<user name>` i `ESX_PASSWORD=<password>`

    Poświadczenia dostępu do serwera vCenter lub hosta ESXi.

`HTTP_PROXY_ADDRESS=<IP address>` i `HTTP_PROXY_PORT=<port>`

Serwer proxy HTTP, którego ma używać agent. W przypadku nieokreślenia tych parametrów serwer proxy nie będzie używany.

`HTTP_PROXY_LOGIN= <login>` i `HTTP_PROXY_PASSWORD=<password>`

Poświadczenia dostępu do serwera proxy HTTP. Jeśli serwer wymaga uwierzytelniania, należy użyć tych parametrów.

`HTTP_PROXY_ONLINE_BACKUP={0,1}`

W przypadku wartości `0` lub nieokreślenia tego parametru agent użyje serwera proxy tylko w przypadku tworzenia kopii zapasowej i odzyskiwania z chmury. W przypadku wartości `1` agent również połączy się z serwerem zarządzania za pośrednictwem serwera proxy.

Parametry dezinstalacji

`REMOVE={ <list of components> |ALL}`

Komponenty do usunięcia oddzielone przecinkami bez spacji. W przypadku wartości `ALL` zostaną odinstalowane wszystkie komponenty produktu.

Ponadto można określić następujący parametr:

`DELETE_ALL_SETTINGS={0, 1}`

W przypadku wartości `1` dzienniki, zadania i ustawienia konfiguracji programu zostaną usunięte.

Przykłady

- Instalowanie agenta dla systemu Windows, narzędzia wiersza polecenia i Monitora cyberochrony. Rejestrowanie komputera w usłudze Cyber Protect przy użyciu nazwy użytkownika i hasła.

  ```
  msiexec.exe /i BackupClient64.msi /l*v my_log.txt /qn
  ADDLOCAL=MmsMspComponents,BackupAndRecoveryAgent,CommandLineTool,TrayMonitor
  TARGETDIR="C:\Program Files\BackupClient" REBOOT=ReallySuppress MMS_USE_SYSTEM_
  ACCOUNT=1 REGISTRATION_ADDRESS=https://cloud.company.com REGISTRATION_LOGIN=johndoe
  REGISTRATION_PASSWORD=johnspassword
  ```

- Instalowanie agenta dla systemu Windows, narzędzia wiersza polecenia i Monitora cyberochrony. Tworzenie nowego konta logowania dla usługi agenta w systemie Windows. Rejestrowanie komputera w usłudze Cyber Protect przy użyciu tokenu.

  ```
  msiexec.exe /i BackupClient64.msi /l*v my_log.txt /qn
  ADDLOCAL=MmsMspComponents,BackupAndRecoveryAgent,CommandLineTool,TrayMonitor
  TARGETDIR="C:\Program Files\BackupClient" REBOOT=ReallySuppress MMS_CREATE_NEW_
  ACCOUNT=1 REGISTRATION_ADDRESS=https://eu2-cloud.company.com REGISTRATION_TOKEN=34F6-
  8C39-4A5C
  ```

- Instalowanie agenta dla systemu Windows, narzędzia wiersza polecenia, agenta dla programu Oracle i Monitora cyberochrony. Rejestrowanie komputera w usłudze Cyber Protect przy użyciu nazwy użytkownika i hasła zakodowanego w formacie base64.

```
msiexec.exe /i BackupClient64.msi /l*v my_log.txt /qn
ADDLOCAL=MmsMspComponents,BackupAndRecoveryAgent,CommandLineTool,OracleAgentFeature,T
rayMonitor TARGETDIR="C:\Program Files\BackupClient" REBOOT=ReallySuppress CURRENT_
LANGUAGE=en MMS_USE_SYSTEM_ACCOUNT=1 REGISTRATION_ADDRESS=https://cloud.company.com
REGISTRATION_LOGIN=johndoe REGISTRATION_PASSWORD_ENCODED=am9obnNwYXNzd29yZA==
```

- Instalowanie agenta dla systemu Windows, narzędzia wiersza polecenia i Monitora cyberochrony. Rejestrowanie komputera w usłudze Cyber Protect przy użyciu tokenu. Ustawienie serwera proxy HTTP.

```
msiexec.exe /i BackupClient64.msi /l*v my_log.txt /qn
ADDLOCAL=MmsMspComponents,BackupAndRecoveryAgent,CommandLineTool,TrayMonitor
TARGETDIR="C:\Program Files\BackupClient" REBOOT=ReallySuppress CURRENT_LANGUAGE=en
MMS_USE_SYSTEM_ACCOUNT=1 REGISTRATION_ADDRESS=https://eu2-cloud.company.com
REGISTRATION_TOKEN=34F6-8C39-4A5C HTTP_PROXY_ADDRESS=https://my-proxy.company.com
HTTP_PROXY_PORT=80 HTTP_PROXY_LOGIN=tomsmith HTTP_PROXY_PASSWORD=tomspassword
```

- Odinstalowywanie wszystkich agentów i usunięcie ich dzienników, zadań oraz ustawień konfiguracyjnych.

```
msiexec.exe /x BackupClient64.msi /l*v uninstall_log.txt REMOVE=ALL DELETE_ALL_
SETTINGS=1 REBOOT=ReallySuppress
```

Instalacja nienadzorowana lub dezinstalacja w systemie Linux

W tej sekcji opisano, jak zainstalować lub odinstalować agenty ochrony w trybie nienadzorowanym na komputerze z systemem Linux przy użyciu wiersza polecenia.

Aby zainstalować lub odinstalować agenta ochrony

1. Otwórz terminal.

2. Wykonaj jedną z następujących czynności:

- Aby rozpocząć instalację przez podanie parametrów w wierszu polecenia, uruchom następujące polecenie:

```
<package name> -a <parameter 1> ... <parameter N>
```

  Zmienna `<nazwa pakietu>` oznacza nazwę pakietu instalacyjnego (pliku .i686 lub .x86_64) Wszystkie dostępne parametry i ich wartości opisano w sekcji „Parametry instalacji nienadzorowanej lub dezinstalacji”.

- Aby rozpocząć instalację z parametrami podanymi w osobnym pliku tekstowym, uruchom następujące polecenie:

```
<package name> -a --options-file=<path to the file>
```

  To rozwiązanie może się przydać, jeśli nie chcesz wprowadzać poufnych informacji w wierszu polecenia. W takiej sytuacji możesz określić ustawienia konfiguracyjne w osobnym pliku

tekstowym i dopilnować, aby nikt inny nie miał do nich dostępu. Umieść każdy parametr w osobnym wierszu wraz z odpowiednią wartością, na przykład:

```
--rain=https://cloud.company.com
--login=johndoe
--password=johnspassword
--auto
```

lub

```
-C
https://cloud.company.com
-g
johndoe
-w
johnspassword
-a
--language
en
```

Jeśli jakiś parametr zostanie określony zarówno w wierszu polecenia, jak i w pliku tekstowym, zostanie użyta wartość z wiersza polecenia.

3. Jeśli na komputerze jest włączona funkcja UEFI Secure Boot, pojawi się informacja o konieczności ponownego uruchomienia systemu po zakończeniu instalacji. Koniecznie zapamiętaj, jakiego hasła (hasła użytkownika root lub „acronis") należy użyć. Podczas ponownego uruchamiania systemu wybierz opcję zarządzania kluczem właściciela komputera, zaznacz **Zarejestruj klucz właściciela komputera**, a następnie zarejestruj klucz przy użyciu zalecanego hasła.

Jeśli po instalacji agenta zostanie włączona funkcja UEFI Secure Boot, powtórz instalację, w tym krok 3. W przeciwnym razie następne operacje tworzenia kopii zapasowej zakończą się niepowodzeniem.

Parametry instalacji nienadzorowanej lub dezinstalacji

W tej sekcji opisano parametry używane podczas instalacji nienadzorowanej lub dezinstalacji w systemie Linux.

Minimalna konfiguracja na potrzeby instalacji nienadzorowanej obejmuje parametr `-a` i parametry rejestracji (na przykład `--login` i `--password`; `--rain` i `--token`). Możesz użyć więcej parametrów, aby dostosować instalację do swoich potrzeb.

Parametry instalacji

Podstawowe parametry

`{-i |--id=}` `<list of components>`

Nazwy komponentów do zainstalowania, rozdzielone przecinkami bez spacji. W pakiecie instalacyjnym .x86_64 dostępne są następujące komponenty do zainstalowania:

Komponent	Opis komponentu
BackupAndRecoveryAgent	Agent dla systemu Linux
AgentForPCS	Agent dla Virtuozzo
OracleAgentFeature	Agent dla programu Oracle

W przypadku nieokreślenia tego parametru zostaną zainstalowane wszystkie powyższe komponenty.

Zarówno agent dla Virtuozzo, jak i agent dla programu Oracle wymagają zainstalowania również agenta dla systemu Linux.

Pakiet instalacyjny .i686 zawiera tylko agenta BackupAndRecoveryAgent.

`{-a|--auto}`

Proces instalacji i rejestracji zostanie zakończony bez dodatkowych działań użytkownika. Korzystając z tego parametru, należy wskazać konto, na którym agent zostanie zarejestrowany w usłudze Cyber Protect — albo przy użyciu parametru `--token`, albo przy użyciu parametrów `--login` i `--password`.

`{-t|--strict}`

W przypadku określenia tego parametru wystąpienie ostrzeżenia podczas instalacji poskutkuje niepowodzeniem instalacji. W przypadku nieokreślenia tego parametru instalacja zostanie pomyślnie ukończona nawet w razie wystąpienia ostrzeżeń.

`{-n|--nodeps}`

Brak wymaganych pakietów systemu Linux zostanie zignorowany podczas instalacji.

`{-d|--debug}`

Dziennik instalacji zostanie zapisany w trybie informacji pełnej.

`--options-file=<location>`

Parametry instalacji zostaną odczytane z pliku tekstowego zamiast z wiersza polecenia.

`--language=<language ID>`

Język programu. Dostępne są następujące wartości: `en, bg, cs, da, de, es, fr, hu, id, it, ja, ko, ms, nb, nl, pl, pt, pt_BR, ru, fi, sr, sv, tr, zh, zh_TW`.
Jeśli ten parametr nie zostanie określony, język produktu zostanie zdefiniowany na podstawie języka systemu, pod warunkiem, że znajduje się on na powyższej liście. Jeśli go nie ma, język produktu zostanie ustawiony na język angielski (`en`).

Parametry rejestracji

Określ jeden z następujących parametrów:

- `{-g|--login=}` `<user name>` i `{-w|--password=}<password>`

  Poświadczenia dostępu do konta, na którym zostanie zarejestrowany agent w usłudze Cyber Protect. Nie może to być konto administratora partnera.

- `--token=` `<token>`

  Token rejestracji to ciąg 12 znaków podzielony dywizami na trzy części. Można go wygenerować w konsoli internetowej <PRODUCT_NAME> zgodnie z instrukcją podaną w sekcji „Wdrażanie agentów przy użyciu zasad grupy”.

  Parametru `--token` nie można używać razem z parametrami `--login`, `--password` i `--register-with-credentials`.

  - `{-C|--rain=}` `<service address>`

    Adres URL usługi Cyber Protect.

    Jeśli do rejestracji zostaną użyte parametry `--login` i `--password`, to nie trzeba jawnie podawać powyższego parametru, ponieważ instalator domyślnie użyje właściwego adresu — tego, którego używasz **do logowania się** do usługi Cyber Protect. Na przykład:

    Jednak w przypadku użycia parametru `{-C|--rain=}` z parametrem `--token` trzeba podać dokładny adres centrum danych. Jest to adres URL widoczny **po zalogowaniu się** do usługi Cyber Protect. Na przykład:

- `--register-with-credentials`

  W przypadku podania tego parametru zostanie uruchomiony graficzny interfejs instalatora. Aby ukończyć rejestrację, należy wprowadzić nazwę użytkownika i hasło do konta, na którym agent zostanie zarejestrowany w usłudze Cyber Protect. Nie może to być konto administratora partnera.

- `--skip-registration`

  Użyj tego parametru, jeśli musisz zainstalować agenta, ale planujesz później go zarejestrować w usłudze Cyber Protect. Więcej informacji o tym, jak to zrobić, można znaleźć w sekcji „Ręczne rejestrowanie komputerów”.

Dodatkowe parametry

`--http-proxy-host=` `<IP address>` i `--http-proxy-port=<port>`

Serwer proxy HTTP, którego agent będzie używać do tworzenia kopii zapasowych lub odzyskiwania z chmury i nawiązywania połączenia z serwerem zarządzania. W przypadku nieokreślenia tych parametrów serwer proxy nie będzie używany.

`--http-proxy-login=` `<login>` i `--http-proxy-password=<password>`

Poświadczenia dostępu do serwera proxy HTTP. Jeśli serwer wymaga uwierzytelniania, należy użyć tych parametrów.

`--tmp-dir= <location>`

Umożliwia wskazanie folderu, w którym mają być przechowywane pliki tymczasowe podczas instalacji. Domyślny folder to **/var/tmp**.

`{-s|--disable-native-shared}`

Podczas instalacji będą używane biblioteki redystrybucyjne, nawet jeśli będą już dostępne w systemie.

`--skip-prereq-check`

Zostanie pominięte sprawdzenie, czy są już zainstalowane pakiety wymagane do skompilowania modułu snapapi.

`--force-weak-snapapi`

Instalator nie będzie kompilował modułu snapapi. Zamiast tego użyje gotowego modułu, który może nie pasować dokładnie do jądra systemu Linux. Odradza się korzystanie z tej opcji.

`--skip-svc-start`

Usługi nie zostaną automatycznie uruchomione po instalacji. Najczęściej parametr ten jest używany z parametrem `--skip-registration`.

Parametry informacyjne

`{-?|--help}`

Umożliwia wyświetlenie opisu parametrów.

`--usage`

Umożliwia wyświetlenie krótkiego opisu zastosowań polecenia.

`{-v|--version}`

Umożliwia wyświetlenie wersji pakietu instalacyjnego.

`--product-info`

Umożliwia wyświetlenie nazwy produktu i wersji pakietu instalacyjnego.

`--snapapi-list`

Umożliwia wyświetlenie dostępnych gotowych modułów snapapi.

`--components-list`

Umożliwia wyświetlenie komponentów instalatora.

Parametry dotyczące starszych funkcji

Te parametry dotyczą starego komponentu agent.exe.

`{-e|--ssl=}` `<path>`

Umożliwia podanie ścieżki do niestandardowego pliku certyfikatu na potrzeby komunikacji SSL.

`{-p|--port=}` `<port>`

Umożliwia wskazanie portu, na którym agent.exe nasłuchuje połączeń. Portem domyślnym jest port 9876.

Parametry dezinstalacji

`{-u|--uninstall}`

Powoduje dezinstalację programu.

`--purge`

Umożliwia odinstalowanie produktu i usunięcie jego dzienników, zadań oraz ustawień konfiguracyjnych. W przypadku korzystania z parametru `--uninstall` nie trzeba jawnie określać parametru `--purge`.

Przykłady

- Instalowanie agenta dla systemu Linux bez rejestrowania go.

  ```
  ./Cyber_Protection_Agent_for_Linux_x86_64.bin -i BackupAndRecoveryAgent -a --skip-registration
  ```

- Instalowanie agenta dla systemu Linux, agenta dla Virtuozzo i agenta dla programu Oracle oraz rejestrowanie ich przy użyciu poświadczeń.

  ```
  ./Cyber_Protection_Agent_for_Linux_x86_64.bin -a --login=johndoe --password=johnspassword
  ```

- Instalowanie agenta dla programu Oracle i agenta dla systemu Linux oraz rejestrowanie ich przy użyciu tokenu rejestracji.

  ```
  ./Cyber_Protection_Agent_for_Linux_x86_64.bin -i BackupAndRecoveryAgent,OracleAgentFeature -a --rain=https://eu2-cloud.company.com --token=34F6-8C39-4A5C
  ```

- Instalowanie agenta dla systemu Linux, agenta dla Virtuozzo i agenta dla programu Oracle przy użyciu ustawień konfiguracyjnych w osobnym pliku tekstowym.

```
./Cyber_Protection_Agent_for_Linux_x86_64.bin -a --options-
file=/home/mydirectory/configuration_file
```

- Odinstalowywanie agenta dla systemu Linux, agenta dla Virtuozzo i agenta dla programu Oracle oraz usuwanie wszystkich ich dzienników, zadań oraz ustawień konfiguracyjnych.

```
./Cyber_Protection_Agent_for_Linux_x86_64.bin -a --purge
```

Nienadzorowane instalowanie i odinstalowywanie w systemie macOS

W tej sekcji opisano, jak zainstalować, zarejestrować i odinstalować agenta ochrony w trybie nienadzorowanym na komputerze z systemem macOS przy użyciu wiersza polecenia. Informacje na temat pobierania pliku instalacyjnego (.dmg) można znaleźć w sekcji „Dodawanie komputera z systemem macOS”.

Aby zainstalować agenta dla systemu Mac

1. Utwórz tymczasowy katalog, w którym zamontujesz plik instalacyjny (.dmg).

   ```
   mkdir <dmg_root>
   ```

   Tutaj `<katalog_główny_dmg>` oznacza dowolną odpowiadającą Ci nazwę.
2. Zamontuj plik .dmg.

   ```
   hdiutil attach <dmg_file> -mountpoint <dmg_root>
   ```

   Tutaj `<plik_dmg>` oznacza nazwę pliku instalacyjnego. Na przykład **AcronisAgentMspMacOSX64.dmg**.
3. Uruchom instalator.

   ```
   sudo installer -pkg <dmg_root>/Install.pkg -target LocalSystem
   ```
4. Odmontuj plik instalacyjny (.dmg).

   ```
   hdiutil detach <dmg_root>
   ```

Przykłady

- ```
  mkdir mydirectory
  ```

  ```
  hdiutil attach /Users/JohnDoe/AcronisAgentMspMacOSX64.dmg -mountpoint mydirectory
  ```

  ```
  sudo installer -pkg mydirectory/Install.pkg -target LocalSystem
  ```

  ```
  hdiutil detach mydirectory
  ```
  ```

Aby zarejestrować agenta dla systemu Mac

Wykonaj jedną z następujących czynności:

- Zarejestruj agenta w ramach określonego konta, podając nazwę użytkownika i hasło.

  ```
  sudo /Library/Application\
  Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent -o register -t cloud -a
  <service address> -u <user name> -p <password>
  ```

  Znaczenie:

  Tutaj `<adres usługi Cyber Protect>` oznacza adres używany w celu **zalogowania się** do usługi Cyber Protect. Na przykład:

  Zmienne `<nazwa użytkownika>` i `<hasło>` to poświadczenia dostępu do konta, w ramach którego zostanie zarejestrowany agent. Nie może to być konto administratora partnera.

- Zarejestruj agenta przy użyciu tokenu rejestracji.

  ```
  sudo /Library/Application\
  Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent -o register -t cloud -a
  <service address> --token <token>
  ```

  Token rejestracji to ciąg 12 znaków podzielony dywizami na trzy części. Można go wygenerować w konsoli internetowej Cyber Protect zgodnie z instrukcją podaną w sekcji „Wdrażanie agentów przy użyciu zasad grupy".

  W przypadku używania tokenu rejestracji trzeba podać dokładny adres centrum danych. Jest to adres URL widoczny **po zalogowaniu się** do usługi Cyber Protect. Na przykład:

Ważne

Jeśli korzystasz z systemu macOS 10.14 lub nowszego, zapewnij agentowi ochrony pełny dostęp do dysku. W tym celu przejdź do sekcji **Aplikacje** > **Narzędzia** i uruchom program **Asystent agenta Cyber Protect Agent**. Następnie postępuj zgodnie z instrukcjami wyświetlanymi w oknie aplikacji.

Przykłady

Rejestracja przy użyciu nazwy użytkownika i hasła.

- ```
  sudo /Library/Application\
  Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent -o register -t cloud -a
  https://cloud.company.com -u johndoe -p johnspassword
  ```

Rejestracja przy użyciu tokenu.
  ```

- ```
  sudo /Library/Application\
  Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent -o register -t cloud -a
  https://eu2-cloud company.com --token D91D-DC46-4F0B
  ```

Aby odinstalować agenta dla systemu Mac

Uruchom następujące polecenie:

- ```
  sudo /Library/Application\ Support/BackupClient/Acronis/Cyber\ Protect\ Agent\
  Uninstall.app/Contents/MacOS/AgentUninstall /confirm
  ```

Aby podczas odinstalowywania usunąć też wszystkie dzienniki, zadania i ustawienia konfiguracyjne, uruchom następujące polecenie:

- ```
  sudo /Library/Application\ Support/BackupClient/Acronis/Cyber\ Protect\ Agent\
  Uninstall.app/Contents/MacOS/AgentUninstall /confirm /purge
  ```

Ręczne rejestrowanie komputerów

Komputer można zarejestrować w usłudze Cyber Protect nie tylko podczas instalacji agenta, ale i przy użyciu interfejsu wiersza polecenia. Może to być konieczne, jeśli agent został zainstalowany, ale na przykład automatyczna rejestracja się nie powiodła lub chcesz zarejestrować istniejący już komputer na nowym koncie.

Aby zarejestrować komputer

W wierszu polecenia komputera, na którym zainstalowany jest agent, uruchom jedno z poniższych poleceń:

- Aby zarejestrować komputer w ramach bieżącego konta:

  ```
  <path to the registration tool> -o register -s mms -t cloud --update
  ```

  - Tutaj `<ścieżka do narzędzia do rejestracji>` oznacza następującą ścieżkę:
    - W systemie Windows: `%ProgramFiles%\BackupClient\RegisterAgentTool\register_agent.exe`
    - W systemie Linux: `/usr/lib/Acronis/RegisterAgentTool/RegisterAgent`
    - W systemie macOS: `/Library/Application Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent`
- Aby zarejestrować komputer w ramach innego konta:

  ```
  <path to the registration tool> -o register -t cloud -a <service address> -u <user
  name> -p <password>
  ```

  - Tutaj zmienne `<nazwa użytkownika>` i `<hasło>` to poświadczenia dostępu do konta, w ramach którego zostanie zarejestrowany agent. Nie może to być konto administratora partnera.
  ```

Zmienna `<adres usługi>` oznacza adres URL używany do **logowania się** do usługi Cyber Protect. Na przykład `https://chmura.nazwa_firmy.com.pl`.

- Aby zarejestrować komputer przy użyciu tokenu rejesracji:

```
<path to the registration tool> -o register -t cloud -a <service address> --token
<token>
```

  - Token rejestracji to ciąg 12 znaków podzielony dywizami na trzy części. Więcej informacji o procedurze generowania tokenu można znaleźć w sekcji „Wdrażanie agentów przy użyciu zasad grupy”.

    W przypadku używania tokenu rejestracji w miejscu zmiennej `<adres usługi>` trzeba podać dokładny adres centrum danych. Jest to adres URL widoczny **po zalogowaniu się** do usługi Cyber Protect. Na przykład `https://eu2-cloud.company.com`.

    W tym przypadku nie używaj `https://cloud.company.com`.

Aby wyrejestrować komputer

W wierszu polecenia komputera, na którym jest zainstalowany agent, uruchom polecenie:

```
<path to the registration tool> -o unregister
```

Przykłady

Windows

```
"%ProgramFiles%\BackupClient\RegisterAgentTool\register_agent.exe" -o register -s mms -t
cloud --update
```

```
"%ProgramFiles%\BackupClient\RegisterAgentTool\register_agent.exe" -o register -t cloud
-a https://cloud.company.com -u johndoe -p johnspassword
```

```
"%ProgramFiles%\BackupClient\RegisterAgentTool\register_agent.exe" -o register -t cloud
-a https://au1-cloud.company.com --token 3B4C-E967-4FBD
```

```
"%ProgramFiles%\BackupClient\RegisterAgentTool\register_agent.exe" -o unregister
```

Linux

```
sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o register -s mms -t cloud --
update
```

```
sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o register -t cloud -a
https://cloud.company.com -u johndoe -p johnspassword
```

```
sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o register -t cloud -a
https://eu2-cloud.company.com --token 34F6-8C39-4A5C
```

```
sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o unregister
```

macOS

```
sudo "/Library/Application Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent"
-o register -s mms -t cloud --update
```

```
sudo "/Library/Application Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent"
-o register -t cloud -a https://cloud.company.com -u johndoe -p johnspassword
```

```
sudo "/Library/Application Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent"
-o register -t cloud -a https://us5-cloud.company.com --token 9DBF-3DA9-4DAB
```

```
sudo "/Library/Application Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent"
-o unregister
```

Hasła ze znakami specjalnymi lub spacjami

Jeśli Twoje hasło zawiera znaki specjalne lub spacje, wpisując je w wierszu polecenia, ujmij je w cudzysłów:

```
<path to the registration tool> -o register -t cloud -a <service address> -u <user name>
-p <"password">
```

Przykład (dotyczący systemu Windows):

```
"%ProgramFiles%\BackupClient\RegisterAgentTool\register_agent.exe" -o register -t cloud
-a https://cloud.company.com -u johndoe -p "johns password"
```

Jeśli nadal pojawia się komunikat o błędzie:

- Zakoduj hasło w formacie base64 na stronie https://www.base64encode.org/.
- W wierszu polecenia podaj zakodowane hasło, używając parametru -b lub --base64.

```
<path to the registration tool> -o register -t cloud -a <service address> -u <user name>
-b -p <encoded password>
```

Przykład (dotyczący systemu Windows):

```
"%ProgramFiles%\BackupClient\RegisterAgentTool\register_agent.exe" -o register -t cloud
-a https://cloud.company.com -u johndoe -b -p am9obnNwYXNzd29yZA==
```

Wdrażanie agenta dla oVirt (urządzenie wirtualne)

Opis wdrażania i konfigurowania agenta dla oVirt (urządzenie wirtualne) można znaleźć w dokumentacji rozwiązania Cyber Protection Cloud.

Wdrażanie agenta dla Virtuozzo Hybrid Infrastructure (urządzenie wirtualne)

Opis wdrażania i konfigurowania agenta dla Virtuozzo Hybrid Infrastructure (urządzenie wirtualne) można znaleźć w dokumentacji rozwiązania Cyber Protection Cloud.

Automatyczne wykrywanie komputerów

Wykrywanie automatyczne umożliwia:

- Automatyzowanie instalacji agentów ochrony i rejestracji komputerów na serwerze zarządzania dzięki funkcji wykrywania komputerów w domenie Active Directory lub sieci lokalnej.
- Instalowanie i aktualizowanie agentów ochrony na wielu komputerach.
- Korzystanie z synchronizacji z domeną Active Directory w celu zmniejszenia nakładu pracy związanej z alokowaniem zasobów i zarządzaniem komputerami w dużej domenie Active Directory.

Wymagania wstępne

Do wykrywania automatycznego potrzebny jest co najmniej jeden komputer z zainstalowanym agentem ochrony w sieci lokalnej lub domenie Active Directory. Agent ten zostanie użyty jako agent wykrywania.

Ważne
Agentami wykrywania mogą być tylko agenty zainstalowane na komputerach z systemem Windows. Jeśli w środowisku nie ma agentów wykrywania, nie będzie można skorzystać z opcji **Wiele urządzeń** w panelu **Dodaj urządzenia**.

Zdalna instalacja agentów jest obsługiwana tylko w przypadku komputerów z systemem Windows (system Windows XP nie jest obsługiwany). Aby dokonać instalacji zdalnej na komputerze z systemem Windows Server 2012 R2, musi na tym komputerze być zainstalowana aktualizacja systemu Windows KB2999226.

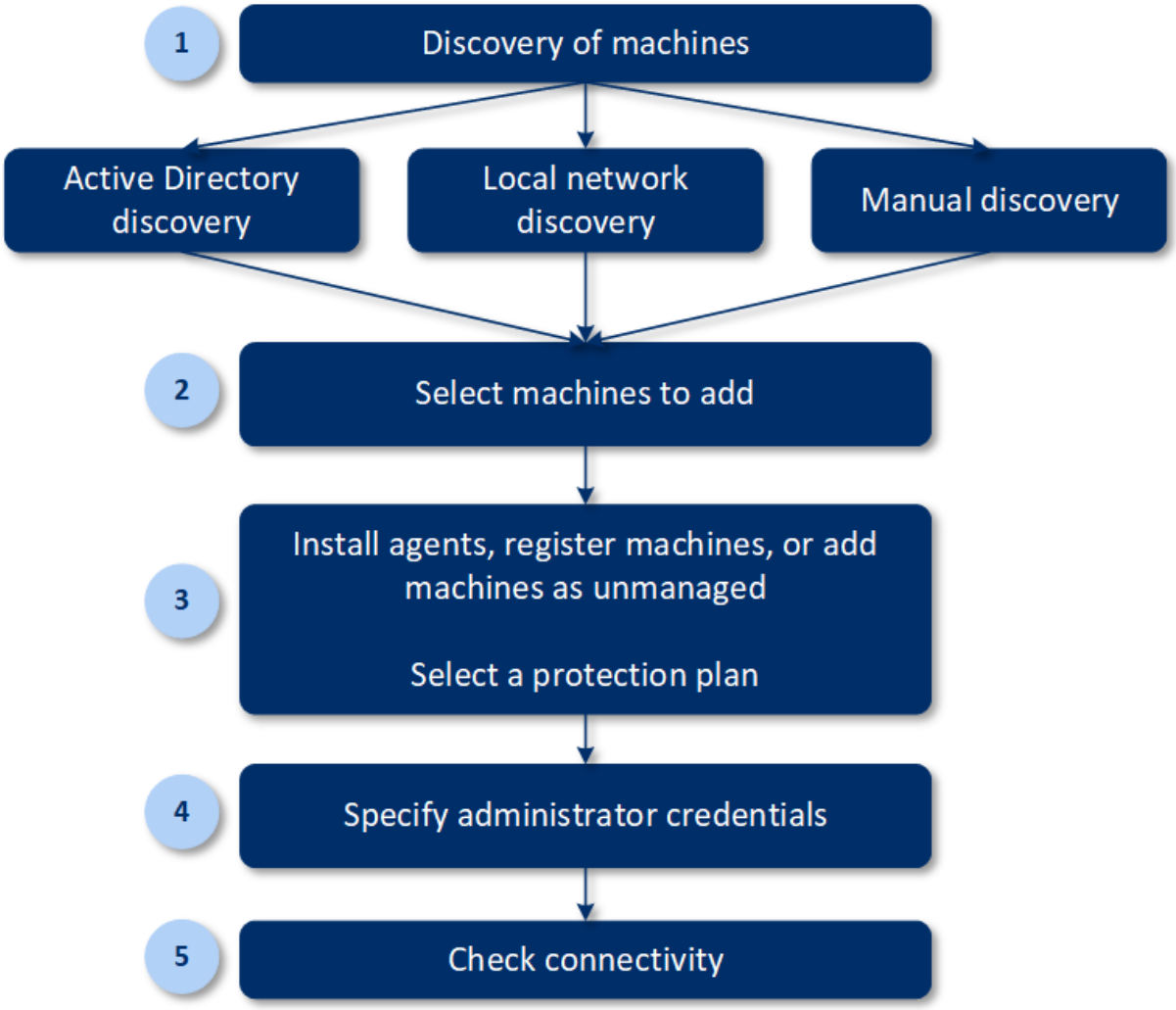
Jak działa wykrywanie automatyczne

Podczas wykrywania w sieci lokalnej agent wykrywania zbiera następujące informacje na temat każdego komputera w sieci, korzystając z funkcji wykrywania NetBIOS, usługi Web Service Discovery (WSD) oraz tabeli Address Resolution Protocol (ARP):

- Nazwa hosta (krótka/NetBIOS)
- W pełni kwalifikowana nazwa domeny (FQDN)
- Domena/grupa robocza
- Adres IPv4/IPv6
- Adres MAC
- System operacyjny (nazwa, wersja, rodzina)
- Kategoria komputera (stacja robocza, serwer, kontroler domeny)

Podczas wykrywania w domenie Active Directory agent wykrywania zbiera informacje z powyższej listy, a także informacje nazwy jednostek organizacyjnych komputerów oraz szczegółowe informacje na temat ich nazw i systemów operacyjnych. Adresy IP ani MAC nie są jednak zbierane.

Poniższy diagram stanowi podsumowanie procesu wykrywania automatycznego.



1. Wybierz metodę wykrywania:
   - Wykrywanie w domenie Active Directory
   - Wykrywanie w sieci lokalnej
   - Wykrywanie ręczne — za pomocą adresu IP lub nazwy hosta komputera albo przez zaimportowanie listy komputerów z pliku

   Wyniki wykrywania w domenie Active Directory lub sieci lokalnej nie obejmują komputerów z zainstalowanymi agentami ochrony.

   W przypadku wykrywania ręcznego istniejące agenty ochrony są aktualizowane i ponownie rejestrowane. W przypadku wykrywania automatycznego przy użyciu tego samego konta, na którym jest zarejestrowany agent, agent zostanie tylko zaktualizowany do najnowszej wersji. W przypadku wykrywania automatycznego przy użyciu innego konta agent zostanie zaktualizowany do najnowszej wersji i ponownie zarejestrowany w ramach dzierżawcy, do którego należy konto.
2. Wybierz komputery, które chcesz dodać do dzierżawcy.
3. Wybierz, jak mają zostać dodane te komputery:
   - Zainstaluj agenta ochrony i dodatkowe komponenty na tych komputerach oraz zarejestruje je w konsoli internetowej.

- Zarejestruj komputery w konsoli internetowej (jeśli agent ochrony jest już zainstalowany).
- Dodaj komputery do konsoli internetowej **Komputery niezarządzane** bez instalowania agenta ochrony.

Można też zastosować już istniejący plan ochrony do komputerów, na których jest instalowany agent ochrony lub które są rejestrowane w konsoli internetowej.

4. Podaj poświadczenia administratora dla wybranych komputerów.
5. Wybierz nazwę lub adres IP serwera zarządzania, których agent będzie używać w celu uzyskania dostępu do tego serwera.

   Domyślnie wybrana jest nazwa serwera. Jeśli serwer zarządzania ma więcej niż jeden interfejs sieciowy lub występują problemy z usługą DNS, które powodują niepowodzenie rejestracji agenta, może być konieczne wybranie adresu IP.
6. Sprawdź, czy możesz nawiązać połączenie z tymi komputerami przy użyciu podanych poświadczeń.

Komputery widoczne w konsoli internetowej Cyber Protect zaliczają się do następujących kategorii:

- **Wykryte** — komputery, które zostały wykryte, ale nie mają zainstalowanego agenta ochrony.
- **Zarządzane** — komputery z zainstalowanym agentem ochrony.
- **Niechronione** — komputery, do których nie zastosowano planu ochrony. W grupie niechronionych komputerów są uwzględniane zarówno wykryte, jak i zarządzane komputery, do których nie zastosowano planu ochrony.
- **Chronione** — komputery, do których zastosowano plan ochrony.

Wykrywanie automatyczne i ręczne

Przed rozpoczęciem operacji wykrywania upewnij się, że zostały spełnione wymagania wstępne.

Aby wykryć komputery

1. W konsoli internetowej przejdź do sekcji **Urządzenia** > **Wszystkie urządzenia**.
2. Kliknij **Dodaj**.
3. W obszarze **Wiele urządzeń** kliknij **Tylko Windows**. Zostanie uruchomiony Kreator wykrywania automatycznego.
4. [Jeśli w organizacji są jednostki] Wybierz jednostkę. Wówczas w polu **Agent wykrywania** będzie można wybrać agenty związane z wybraną jednostką i jej jednostkami podrzędnymi.
5. Wybierz agenta wykrywania, który ma przeprowadzić skanowanie w celu wykrycia komputerów.
6. Wybierz metodę wykrywania:
   - **Szukaj w usłudze Active Directory**. Upewnij się, że komputer z agentem wykrywania należy do domeny Active Directory.
   - **Skanuj sieć lokalną**. Jeśli wybrany agent wykrywania nie znajdzie żadnego komputera, wybierz innego agenta wykrywania.

- **Wpisz ręcznie lub zaimportuj z pliku**. Ręcznie zdefiniuj komputery, które mają zostać dodane, lub zaimportuj je z pliku tekstowego.

7. [Jeśli wybrano metodę wykrywania w domenie Active Directory] Wybierz sposób wyszukiwania komputerów:
   - **Na liście jednostek organizacyjnych**. Wybierz grupę komputerów, które mają zostać dodane.
   - **Według zapytania w dialekcie LDAP**. Użyj zapytania w dialekcie LDAP, aby wybrać komputery. Opcja **Baza wyszukiwania** umożliwia określenie przeszukiwanych miejsc, a pole **Filtruj** umożliwia podanie kryteriów wyboru komputerów.
8. [Jeśli wybrano metodę wykrywania w domenie Active Directory lub sieci lokalnej] Użyj listy, aby wybrać komputery, które chcesz dodać.

   [Jeśli wybrano metodę wykrywania ręcznego] Podaj adresy IP lub nazwy hostów komputerów albo zaimportuj listę komputerów z pliku tekstowego. Plik musi zawierać adresy IP / nazwy hostów — każdy w osobnym wierszu. Przykładowy plik:

   ```
   156.85.34.10
   156.85.53.32
   156.85.53.12
   EN-L00000100
   EN-L00000101
   ```

   Po ręcznym dodaniu adresów komputerów lub zaimportowaniu ich z pliku agent próbuje wysłać do dodanych komputerów polecenia ping i ustalić ich dostępność.
9. Określ, co ma zostać zrobione po zakończeniu operacji wykrywania:
   - **Zainstaluj agenty i zarejestruj komputery**. Możesz wybrać komponenty, które mają zostać zainstalowane na komputerach, klikając **Wybierz komponenty**. Więcej informacji można znaleźć w sekcji „Wybieranie komponentów do zainstalowania”. Można zainstalować do 100 agentów naraz.

     Na ekranie **Wybierz komponenty** wskaż konto, na którym będą działać usługi, w polu **Konto logowania dla usługi agenta**. Można wybrać jedną z następujących opcji:
     - **Użyj kont użytkowników usługi** (domyślne w przypadku usługi agenta)

       Konta użytkowników usługi to konta w systemie Windows używane do uruchamiania usług. Ustawienie to ma tę zaletę, że zasady zabezpieczeń domeny nie wpływają na prawa użytkowników tych kont. Domyślnie agent działa na koncie **System lokalny**.
     - **Utwórz nowe konto**

       Nazwą konta dla danego agenta będzie Agent User.
     - **Użyj następującego konta**

       Jeśli agent zostanie zainstalowany na kontrolerze domeny, system wyświetli monit o określenie istniejących już kont (lub tego samego konta) na potrzeby agenta. Ze względów bezpieczeństwa system nie tworzy automatycznie nowych kont na kontrolerze domeny.

     W przypadku wybrania opcji **Utwórz nowe konto** lub **Użyj następującego konta** dopilnuj, aby zasady zabezpieczeń domeny nie wpływały na prawa powiązanych kont. Jeśli konto straci

prawa użytkownika przypisane podczas instalacji, komponent może działać niepoprawnie lub wcale nie działać.

- **Zarejestruj komputery z zainstalowanymi agentami**. Ta opcja jest używana, jeśli agent jest już zainstalowany na komputerach i wystarczy go zarejestrować w usłudze Cyber Protect. Jeśli na komputerach nie zostanie znaleziony żaden agent, zostaną one dodane jako komputery **Niezarządzane**.
- **Dodaj jako komputery niezarządzane**. Agent nie zostanie zainstalowany na tych komputerach. Będzie można je przeglądać w konsoli internetowej i zainstalować lub zarejestrować danego agenta później.

[W przypadku wybrania opcji **Zainstaluj agenty i zarejestruj komputery** jako działania po wykryciu] **W razie potrzeby uruchom ponownie komputer** — w przypadku włączenia tej opcji komputer zostanie uruchomiony ponownie tyle razy, ile będzie trzeba w celu ukończenia instalacji.

Ponowne uruchomienie komputera może być wymagane w jednym z poniższych przypadków:

- Ukończono instalację oprogramowania określonego w wymaganiach wstępnych instalacji i trzeba uruchomić ponownie komputer, aby kontynuować instalację.
- Ukończono instalację, ale trzeba uruchomić ponownie komputer, ponieważ niektóre pliki zostały zablokowane na czas instalacji.
- Ukończono instalację, ale trzeba uruchomić ponownie komputer ze względu na inne wcześniej zainstalowane oprogramowanie.

[W przypadku wybrania opcji **W razie potrzeby uruchom ponownie komputer**] **Nie uruchamiaj ponownie komputera, jeśli jest zalogowany użytkownik** — w przypadku włączenia tej opcji komputer nie zostanie automatycznie uruchomiony ponownie, jeśli użytkownik jest zalogowany w systemie. Jeśli na przykład użytkownik pracuje w czasie, gdy instalacja wymaga ponownego uruchomienia systemu, operacja ta nie zostanie wykonana.

Jeśli zostały spełnione warunki wstępne, po czym z powodu zalogowania użytkownika nie uruchomiono ponownie komputera, to w celu ukończenia instalacji agenta trzeba będzie uruchomić ponownie komputer i na nowo rozpocząć instalację.

Jeśli agent został zainstalowany, ale nie uruchomiono ponownie komputera, należy tę operację wykonać.

[Jeśli organizacja ma jednostki] **Jednostka, w której mają zostać zarejestrowane komputery** — wybierz jednostkę, w której zostaną zarejestrowane komputery.

W przypadku wybrania jednego z dwóch pierwszych działań po wykryciu można też zastosować do komputerów plan ochrony. Jeśli masz kilka planów ochrony, możesz wybrać jeden z nich.

10. Podaj poświadczenia użytkownika, który ma prawa administratora do wszystkich dodanych komputerów.

Ważne
Należy pamiętać, że zdalna instalacja agenta działa bez żadnych przygotowań tylko w przypadku podania poświadczeń dostępu do wbudowanego konta administratora (pierwszego konta utworzonego podczas instalacji systemu operacyjnego). Aby zdefiniować poświadczenia dla administratora niestandardowego, należy wykonać dodatkowe czynności przygotowawcze ręcznie, zgodnie z opisem podanym w sekcji Dodawanie komputera z systemem Windows > Przygotowanie.

11. Wybierz nazwę lub adres IP serwera zarządzania, których agent będzie używać w celu uzyskania dostępu do tego serwera.
    Domyślnie wybrana jest nazwa serwera. Jeśli serwer zarządzania ma więcej niż jeden interfejs sieciowy lub występują problemy z usługą DNS, które powodują niepowodzenie rejestracji agenta, może być konieczne wybranie adresu IP.
12. System sprawdza możliwość nawiązania połączenia ze wszystkimi komputerami. Jeśli w przypadku jakichś komputerów połączenie się nie powiedzie, można zmienić dotyczące ich poświadczenia.

Po zainicjowaniu operacji wykrywania komputerów odpowiednie zadanie można znaleźć w działaniu **Panel** > **Działania** > **Wykrywanie komputerów**.

Wybieranie komponentów do zainstalowania

Poniższa tabela zawiera opisy wymaganych i dodatkowych komponentów:

Komponent	Opis
Wymagany komponent	
Agent dla systemu Windows	Ten agent tworzy kopie zapasowe dysków, woluminów i plików. Jest instalowany na komputerach z systemem Windows. Zawsze zostanie zainstalowany — brak możliwości wyboru.
Dodatkowe komponenty	
Agent dla Hyper-V	Ten agent tworzy kopie zapasowe maszyn wirtualnych Hyper-V. Jest instalowany na hostach Hyper-V. Zostanie zainstalowany w przypadku wybrania takiej opcji i wykrycia na komputerze roli Hyper-V.
Agent dla SQL	Ten agent tworzy kopie zapasowe baz danych programu SQL Server. Jest instalowany na komputerach z programem Microsoft SQL Server. Zostanie zainstalowany w przypadku wybrania takiej opcji i wykrycia programu na komputerze.
Agent dla programu Exchange	Ten agent tworzy kopie zapasowe baz danych programu Exchange. Jest instalowany na komputerach z rolą Skrzynka pocztowa

	programu Microsoft Exchange Server. Zostanie zainstalowany w przypadku wybrania takiej opcji i wykrycia programu na komputerze.
Agent dla usługi Active Directory	Ten agent tworzy kopie zapasowe danych Usług domenowych Active Directory. Jest instalowany na kontrolerach domen. Zostanie zainstalowany w przypadku wybrania takiej opcji i wykrycia programu na komputerze.
Agent dla VMware (Windows)	Ten agent tworzy kopie zapasowe maszyn wirtualnych VMware. Jest instalowany na komputerach z systemem Windows, które mają dostęp sieciowy do serwera vCenter. Zostanie zainstalowany w przypadku wybrania takiej opcji.
Agent dla usługi Office 365	Ten agent tworzy kopie zapasowe skrzynek pocztowych pakietu Microsoft 365 w lokalnym miejscu docelowym. Jest instalowany na komputerach z systemem Windows. Zostanie zainstalowany w przypadku wybrania takiej opcji.
Agent dla programu Oracle	Ten agent tworzy kopie zapasowe baz danych Oracle. Jest instalowany na komputerach z oprogramowaniem Oracle Database. Zostanie zainstalowany w przypadku wybrania takiej opcji.
Cyber Protect Monitor	Ten komponent umożliwia użytkownikowi monitorowanie wykonywania uruchomionych zadań w obszarze powiadomień. Jest instalowany na komputerach z systemem Windows. Zostanie zainstalowany w przypadku wybrania takiej opcji.
Narzędzie wiersza polecenia	Usługa Cyber Protect obsługuje interfejs wiersza polecenia za pomocą programu narzędziowego acrocmd. Program acrocmd nie zawiera żadnych narzędzi fizycznie wykonujących polecenia. On jedynie udostępnia interfejs wiersza polecenia komponentom usługi Cyber Protect — agentom oraz serwerowi zarządzania. Zostanie zainstalowany w przypadku wybrania takiej opcji.
Generator nośnika startowego	Ten komponent umożliwia użytkownikom tworzenie nośników startowych. Jest instalowany na komputerach z systemem Windows (jeśli zostanie wybrany).

Zarządzanie wykrytymi komputerami

Po zakończeniu procesu wykrywania wszystkie wykryte komputery można znaleźć w sekcji **Urządzenia** > **Komputery niezarządzane**.

Sekcja ta jest podzielona na podsekcje według zastosowanej metody wykrywania. Oto pełna lista parametrów komputerów (mogą być różne w zależności od metody wykrywania):

Nazwa	Opis
Nazwa	Nazwa komputera. Jeśli nie wykryto nazwy komputera, będzie

	wyświetlany jego adres IP.
Adres IP	Adres IP komputera.
Typ wykrywania	Metoda wykrywania zastosowana w celu wykrycia maszyny.
Jednostka organizacyjna	Jednostka organizacyjna w domenie Active Directory, do której należy komputer. Ta kolumna jest wyświetlana w przypadku przeglądania listy komputerów w sekcji **Komputery niezarządzane** > **Active Directory**.
System operacyjny	System operacyjny zainstalowany na komputerze.

W sekcji **Wyjątki** można dodać komputery, które mają zostać pominięte podczas wykrywania. Jeśli na przykład nie potrzebujesz, być któreś komputery zostały wykryte, możesz je dodać do tej listy.

Aby dodać komputer w sekcji **Wyjątki**, zaznacz go na liście i kliknij **Dodaj do wyjątków**. Aby usunąć komputer z sekcji **Wyjątki**, przejdź do sekcji **Komputery niezarządzane** > **Wyjątki**, zaznacz komputer i kliknij **Usuń z wyjątków**.

Możesz zainstalować agenta ochrony i zarejestrować grupę wykrytych komputerów w usłudze Cyber Protect — w tym celu zaznacz je na liście i kliknij **Zainstaluj i zarejestruj**. Otwarty kreator pozwala również na przypisanie planu ochrony do grupy komputerów.

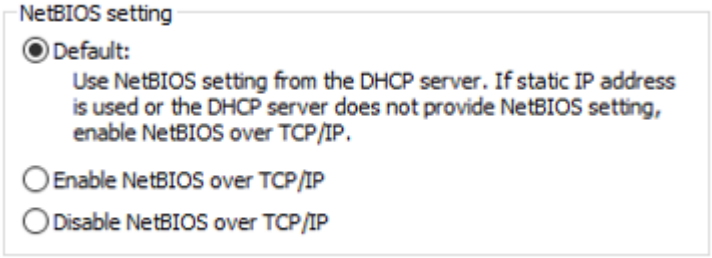
Po zainstalowaniu na komputerach agenta ochrony komputery te będą widoczne w sekcji **Urządzenia** > **Komputery z agentami**.

Aby sprawdzić status ochrony, przejdź do sekcji **Panel** > **Przegląd** i dodaj widżet **Status ochrony** lub **Wykryty komputer**.

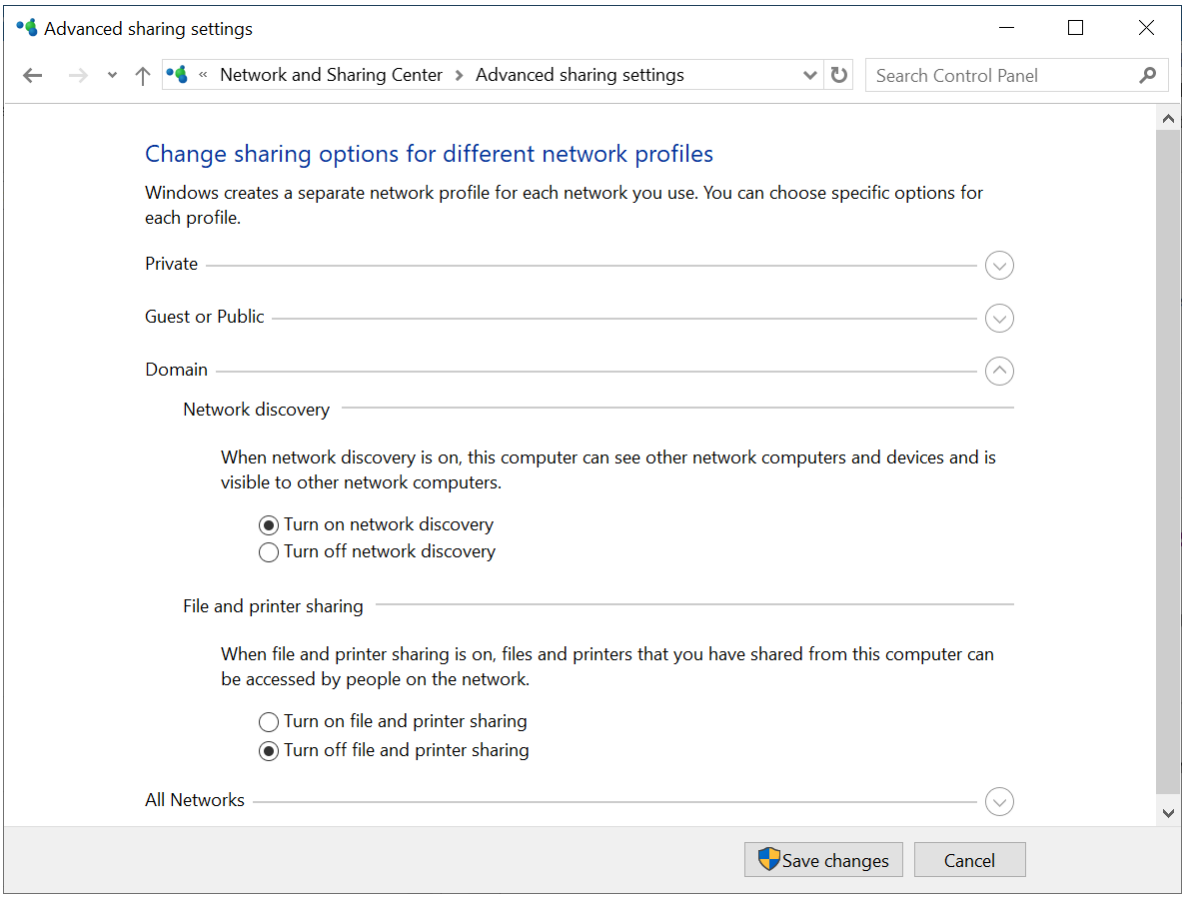
Rozwiązywanie problemów

W razie jakichkolwiek problemów z funkcją automatycznego wykrywania spróbuj podjąć następujące kroki:

- Sprawdź, czy jest włączony lub ustawiony jako domyślny protokół NetBIOS over TCP/IP.



- W sekcji **Panel sterowania** > **Centrum sieci i udostępniania** > **Zaawansowane ustawienia udostępniania** włącz Odnajdowanie sieci.



- Sprawdź, czy na komputerze obsługującym wykrywanie oraz komputerach, które mają zostać wykryte, działa usługa **Host dostawcy odnajdowania funkcji**.
- Sprawdź, czy na komputerach, które mają zostać wykryte, działa usługa **Publikacja zasobów odnajdowania funkcji**.

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

Zanim zaczniesz

Wymagania systemowe agenta

Domyślnie urządzeniu wirtualnemu przydzielane jest 4 GB pamięci RAM oraz dwa procesory vCPU, co jest optymalne i wystarczające dla większości operacji. Zalecamy zwiększenie tych zasobów do 8 GB RAM i 4 procesorów vCPU, jeśli ruch w sieci związany z tworzeniem kopii zapasowych może przekroczyć 100 MB na sekundę (na przykład w sieciach 10 Gb/s), aby podnieść wydajność tworzenia kopii zapasowej.

Własne dyski wirtualne urządzenia zajmują nie więcej niż 6 GB. Format dysku („gruby” czy „chudy”) nie ma wpływu na wydajność urządzenia.

Uwaga
Interfejsy vStorage API muszą być zainstalowane na hoście ESXi, aby można było tworzyć kopie zapasowe maszyn wirtualnych. Zobacz https://kb.acronis.com/content/14931.

Ile agentów potrzebuję?

Mimo iż jedno urządzenie wirtualne jest w stanie chronić całe środowisko vSphere, najlepsza praktyka zakłada użycie jednego urządzenia wirtualnego na każdy klaster vSphere (lub hosta w przypadku braku klastrów). Pozwala to na szybsze tworzenie kopii zapasowych, ponieważ urządzenie może podłączyć dyski uwzględniane w kopiach zapasowych przy użyciu transportu HotAdd, w związku z czym ruch związany z tworzeniem kopii zapasowych jest kierowany z jednego dysku lokalnego na drugi.

Normalną praktyką jest jednoczesne korzystanie z urządzenia wirtualnego i Agent dla VMware (Windows), o ile są one podłączone do tego samego serwer vCenter *lub* do innych hostów ESXi. Należy unikać sytuacji, w której jeden agent podłączony jest bezpośrednio do ESXi, a drugi agent jest podłączony do serwera vCenter zarządzającego tym ESXi.

Nie zalecamy korzystania z magazynu dołączonego lokalnie (tj. przechowywania kopii zapasowych na dyskach wirtualnych dodanych do urządzenia wirtualnego) w przypadku korzystania z więcej niż jednego agenta. Aby uzyskać więcej informacji, patrz „Używanie magazynu dołączonego lokalnie”.

Wyłączanie automatycznego harmonogramu zasobów rozproszonych (Distributed Resource Scheduler —DRS) dla agenta

Jeśli w klastrze vSphere zostało wdrożone urządzenie wirtualne, należy wyłączyć dla niego automatyczne narzędzie vMotion. W ustawieniach DRS klastra włącz poziomy automatyzacji konkretnej maszyny wirtualnej, a następnie ustaw **Poziom automatyzacji** dla urządzenia wirtualnego jako **Wyłączony**.

Wdrażanie szablonu OVF

Lokalizacja szablonu OVF

Szablon OVF obejmuje jeden plik .ovf i dwa pliki .vmdk.

W ramach wdrożeń lokalnych

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).

W ramach wdrożeń w chmurze

1. Kliknij **Wszystkie urządzenia** > **DodajVMware ESXi** > **Urządzenie wirtualne (OVF)**.
   Na Twoją maszynę zostanie pobrane archiwum zip.

2. Rozpakuj archiwum .zip.

Wdrażanie szablonu OVF

1. Dopilnuj, aby z komputera z klientem vSphere można było uzyskać dostęp do plików szablonu OVF.
2. Uruchom klienta vSphere i zaloguj się na serwerze vCenter.
3. Wdróż szablon OVF.
   - Przy konfiguracji magazynu danych wybierz współdzielony magazyn danych, jeśli taki istnieje. Format dysku („gruby" czy „chudy") nie ma wpływu na wydajność urządzenia.
   - Konfigurując połączenia sieciowe w przypadku wdrożeń w chmurze, wybierz sieć, która umożliwia połączenie z Internetem, tak aby agent mógł poprawnie zarejestrować się w chmurze. Konfigurując połączenia sieciowe w przypadku wdrożenia lokalnego, wybierz sieć, w której się znajduje serwer zarządzania.

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).
2. **Serwer proxy**

   Jeśli w sieci jest włączony serwer proxy:
   a. Aby uruchomić powłokę poleceń, naciśnij CTRL+SHIFT+F2 w interfejsie użytkownika urządzenia wirtualnego.
   b. Otwórz plik **/etc/Acronis/Global.config** w edytorze tekstowym.
   c. Wykonaj jedną z następujących czynności:
      - Jeśli ustawienia serwera proxy zostały określone podczas instalacji agenta, znajdź następującą sekcję:

        ```
        <key name="HttpProxy">
            <value name="Enabled" type="Tdword">"1"</value>
            <value name="Host" type="TString">"ADDRESS"</value>
            <value name="Port" type="Tdword">"PORT"</value>
            <value name="Login" type="TString">"LOGIN"</value>
            <value name="Password" type="TString">"PASSWORD"</value>
        </key>
        ```

      - W przeciwnym wypadku skopiuj powyższe wiersze i wklej je do pliku między znacznikami `<registry name="Global">...</registry>`.

   d. Zastąp wartość `ADRES` nową nazwą hosta / adresem IP serwera proxy, a wartość `PORT` — wartością dziesiętną numeru portu.
   e. Jeśli serwer proxy wymaga uwierzytelnienia, zastąp `NAZWA LOGOWANIA` i `HASŁO` poświadczeniami serwera proxy. W przeciwnym razie usuń te wiersze z pliku.

f. Zapisz plik.

g. Otwórz plik **/opt/acronis/etc/aakore.yaml** w edytorze tekstów.

h. Znajdź sekcję **env** lub ją utwórz i dodaj następujące wiersze:

```
env:
 http-proxy: proxy_login:proxy_password@proxy_address:port
 https-proxy: proxy_login:proxy_password@proxy_address:port
```

i. Zastąp zmienne `nazwa_logowania_proxy` i `hasło_proxy` poświadczeniami dostępu do serwera proxy, a zmienną `adres_proxy:port` — adresem i numerem portu serwera proxy.

j. Uruchom polecenie **`reboot`**.

W przeciwnym razie pomiń ten krok.

3. **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.

4. **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.

   Podaj 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 na serwerze vCenter lub ESXi.

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

5. **Serwer zarządzania**

   a. W obszarze **Opcje agenta**, w polu **Serwer zarządzania** kliknij **Zmień**.

   b. W polu **Nazwa / adres IP serwera** wykonaj jedną z następujących czynności:

   - W przypadku wdrożenia lokalnego wybierz **Lokalne**. Określ nazwę hosta lub adresIP komputera, na którym jest zainstalowany serwer zarządzania.
   - W przypadku wdrożenia w chmurze wybierz **Chmura**. W oprogramowaniu zostanie wyświetlony adres usługi Cyber Protection. Nie zmieniaj tego adresu, chyba że otrzymasz inne instrukcje.

   c. W polach **Nazwa użytkownika** i **Hasło** wykonaj jedną z następujących czynności:

   - W przypadku wdrożenia lokalnego podaj nazwę użytkownika i hasło administratora serwera zarządzania.

- W przypadku wdrożenia w chmurze podaj nazwę użytkownika i hasło usługi Cyber Protection. Agent i maszyny wirtualne zarządzane przez agenta zostaną zarejestrowane na tym koncie.

6. **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.

7. **[Opcjonalnie] Magazyny lokalne**

   Do urządzenia wirtualnego można podłączyć dodatkowy dysk, aby agent dla VMware mógł tworzyć kopie zapasowe w takim lokalnie podłączonym magazynie.

   Dodaj dysk, edytując ustawienia maszyny wirtualnej, i kliknij **Odśwież**. Łącze **Utwórz magazyn** stanie się dostępne. Kliknij je, wybierz dysk i określ jego etykietę.

Wdrażanie agenta dla Scale Computing HC3 (urządzenie wirtualne)

Zanim zaczniesz

Urządzenie to jest prekonfigurowaną maszyną wirtualną, którą użytkownik wdraża w klastrze Scale Computing HC3. Zawiera ono agenta ochrony, który pozwala na administrowanie cyberochroną wszystkich maszyn wirtualnych w klastrze.

Wymagania systemowe agenta

Podczas wdrażania urządzenia wirtualnego można wybrać odpowiednią opcję spośród różnych kombinacji procesorów vCPU i pamięci RAM. W przypadku większości operacji optymalną i wystarczającą kombinacją są 2 procesory vCPU oraz 4 GB pamięci RAM. Jeśli ruch w sieci związany z tworzeniem kopii zapasowych może przekroczyć 100 MB na sekundę (na przykład w sieciach 10 Gb/s), warto zwiększyć zasoby do 4 procesorów vCPU i 8 GB pamięci RAM, aby poprawić wydajność tworzenia kopii zapasowych.

Własne dyski wirtualne urządzenia zajmują nie więcej niż 6 GB.

Ile agentów potrzebuję?

Jeden agent może chronić cały klaster. Jeśli jednak trzeba rozłożyć obciążenie sieci ruchem związanym z tworzeniem kopii zapasowych, można mieć więcej niż jednego agenta w klastrze.

W przypadku dostępności więcej niż jednego agenta w klastrze, maszyny wirtualne są automatycznie po równo przydzielane agentom, tak aby każdy z nich zarządzał taką samą liczbą maszyn.

Za każdym razem, gdy różnica obciążenia między agentami przekracza 20 procent, następuje ponowny automatyczny przydział. Może się tak zdarzyć na przykład w przypadku dodania bądź usunięcia jednego z komputerów lub agentów. Przykład: zauważasz potrzebę podłączenia większej

liczby agentów w celu zwiększenia przepustowości i wdrażasz w klastrze dodatkowe urządzenie wirtualne. Serwer zarządzania przypisze najbardziej odpowiednie maszyny nowemu agentowi. Zmniejszy się obciążenie starszych agentów. W przypadku usunięcia agenta z serwera zarządzania komputery przypisane temu agentowi zostaną przydzielone pozostałym agentom. Nie jest to jednak możliwe w przypadku uszkodzenia agenta lub jego ręcznego usunięcia z klastra Scale Computing HC3. Proces ponownego przydzielania rozpocznie się dopiero po usunięciu takiego agenta z interfejsu internetowego usługi Cyber Protect.

Można sprawdzić wynik automatycznej dystrybucji:

- W kolumnie **Agent** w przypadku każdej maszyny wirtualnej w sekcji **Wszystkie urządzenia**
- W sekcji **Przypisane maszyny wirtualne** panelu **Szczegóły**, kiedy agent jest zaznaczony w sekcji **Ustawienia** > **Agenci**

Wdrażanie urządzenia wirtualnego

1. Zaloguj się na koncie Cyber Protect.
2. Kliknij **Urządzenia** > **Wszystkie urządzenia** > **Dodaj** > **Scale Computing HC3**.
3. Wybierz liczbę urządzeń wirtualnych, które chcesz wdrożyć.
4. Podaj adres IP lub nazwę hosta klastra Scale Computing HC3.
5. Podaj poświadczenia dostępu do konta z przypisaną rolą **VM Create/Edit** (Tworzenie/edycja maszyn wirtualnych) w tym klastrze.
6. Wskaż udział sieciowy, który będzie używany do tymczasowego przechowywania pliku obrazu urządzenia wirtualnego. Wymagane jest minimum 2 GB wolnego miejsca.
7. Podaj poświadczenia dostępu do konta z uprawnieniami do odczytu i zapisu do tego udziału sieciowego.
8. Kliknij **Wdróż**.

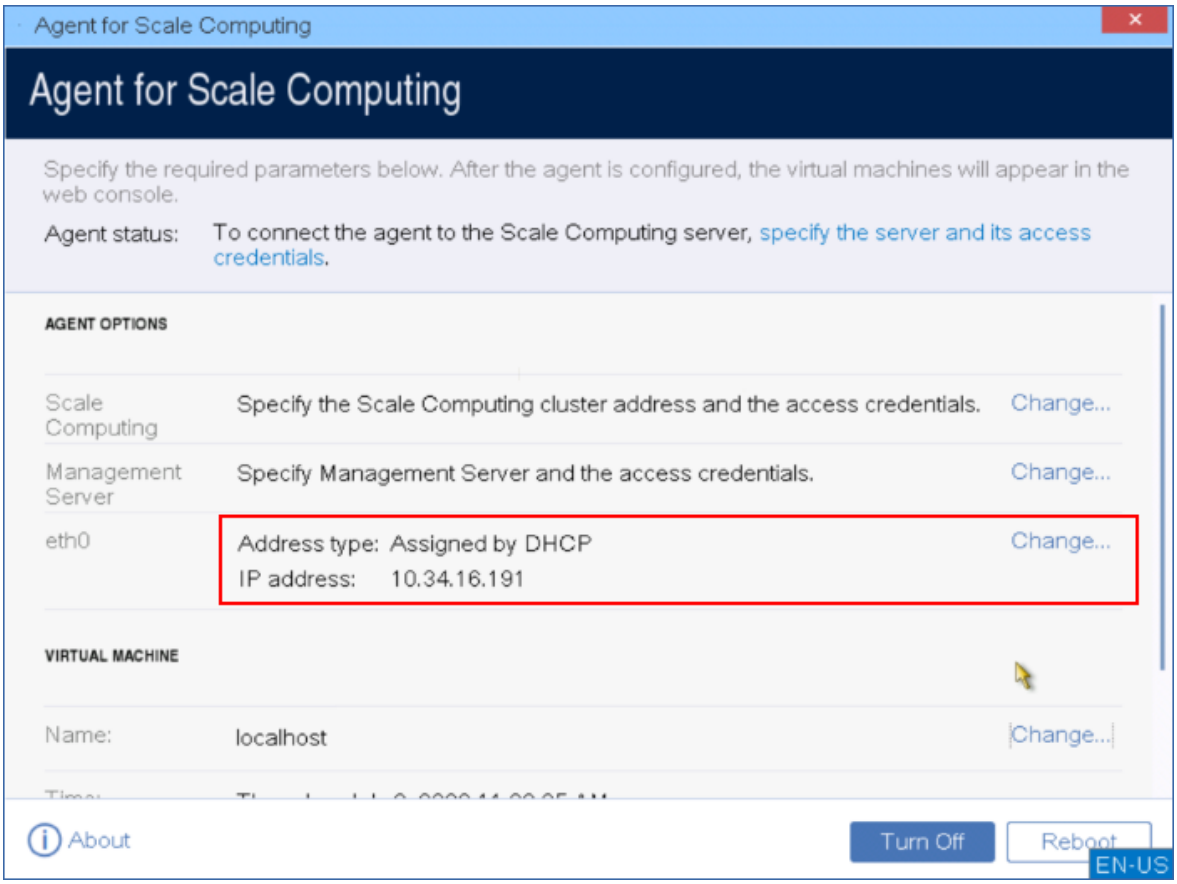
Po zakończeniu operacji wdrożenia skonfiguruj urządzenie wirtualne.

Konfigurowanie urządzenia wirtualnego

Po wdrożeniu urządzenia wirtualnego należy je skonfigurować tak, aby miało dostęp zarówno do klastra Scale Computing HC3, który ma ono chronić, jak i do serwera zarządzania Cyber Protect.

Aby skonfigurować urządzenie wirtualne

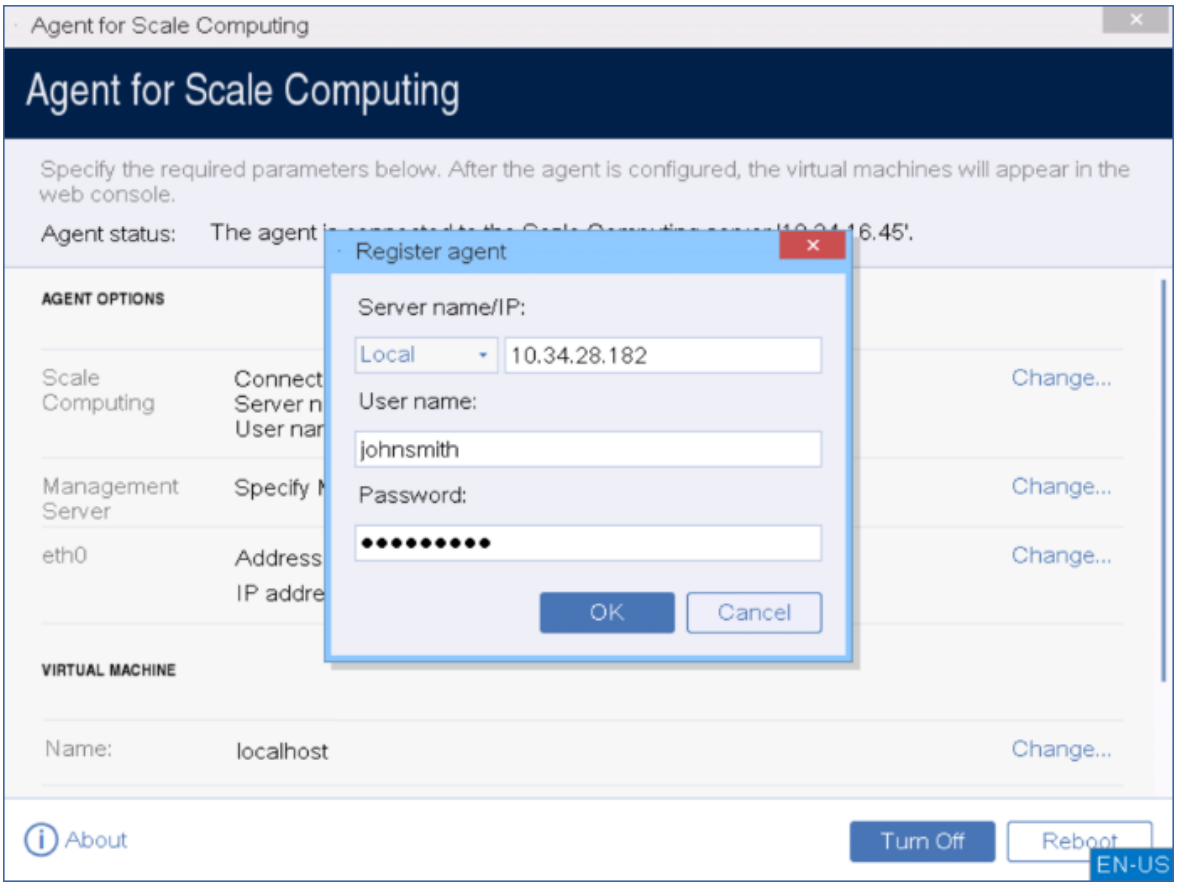
1. Zaloguj się na koncie Scale Computing HC3.
2. Wybierz maszynę wirtualną z agentem, którego chcesz skonfigurować, a następnie kliknij **Konsola**.
3. Skonfiguruj interfejsy sieciowe urządzenia. Może być jeden lub kilka interfejsów do skonfigurowania — to zależy to od liczby sieci, z których korzysta urządzenie. Upewnij się, że automatycznie przypisane adresy DHCP (jeśli zostały użyte) są prawidłowe w sieciach, z których korzysta Twoja maszyna wirtualna, lub przypisz je ręcznie.



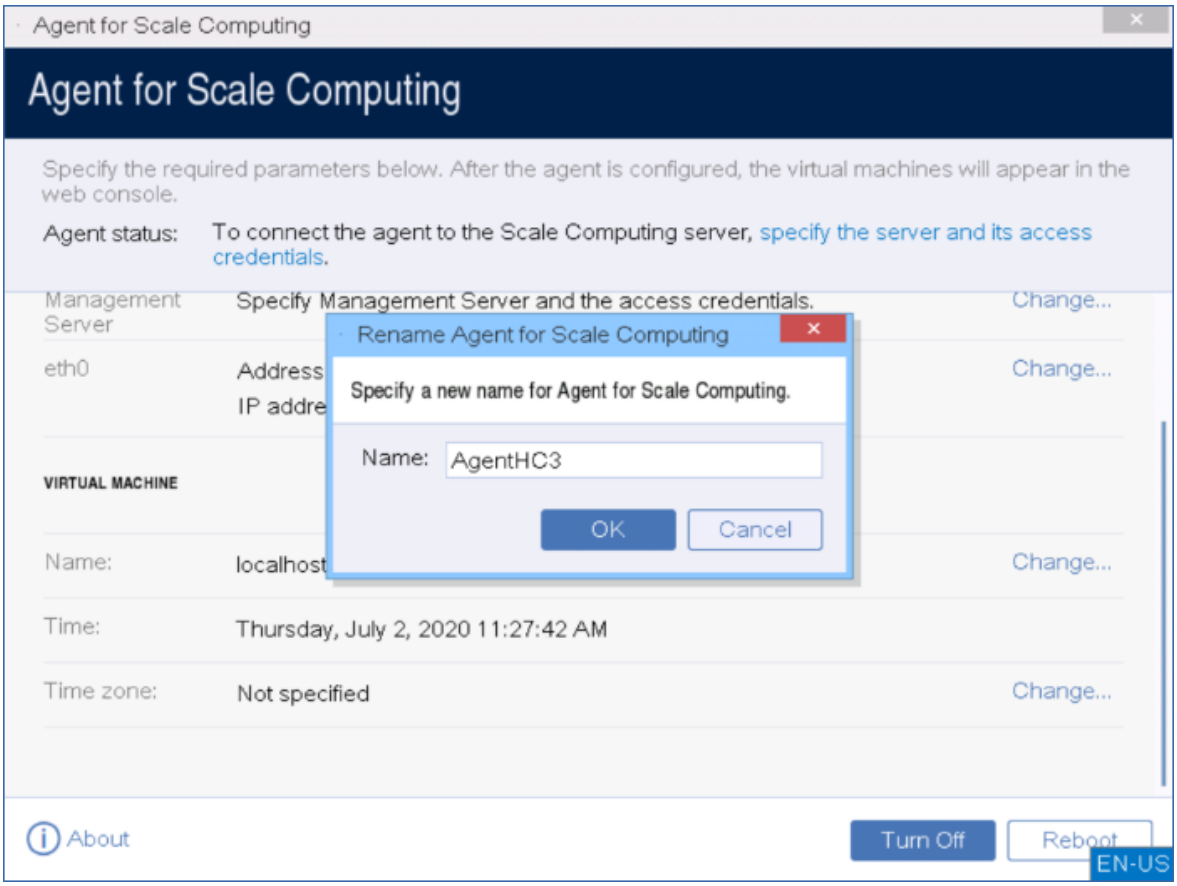
4. Podaj adres klastra Scale Computing HC3 i poświadczenia:
   - Nazwa DNS lub adres IP klastra.
   - W polach **Nazwa użytkownika** i **Hasło** wprowadź poświadczenia dostępu do konta w środowisku Scale Computing HC3 mającego przypisane odpowiednie role.

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

5. Podaj adres serwera zarządzania Cyber Protect i poświadczenia dostępu do niego.



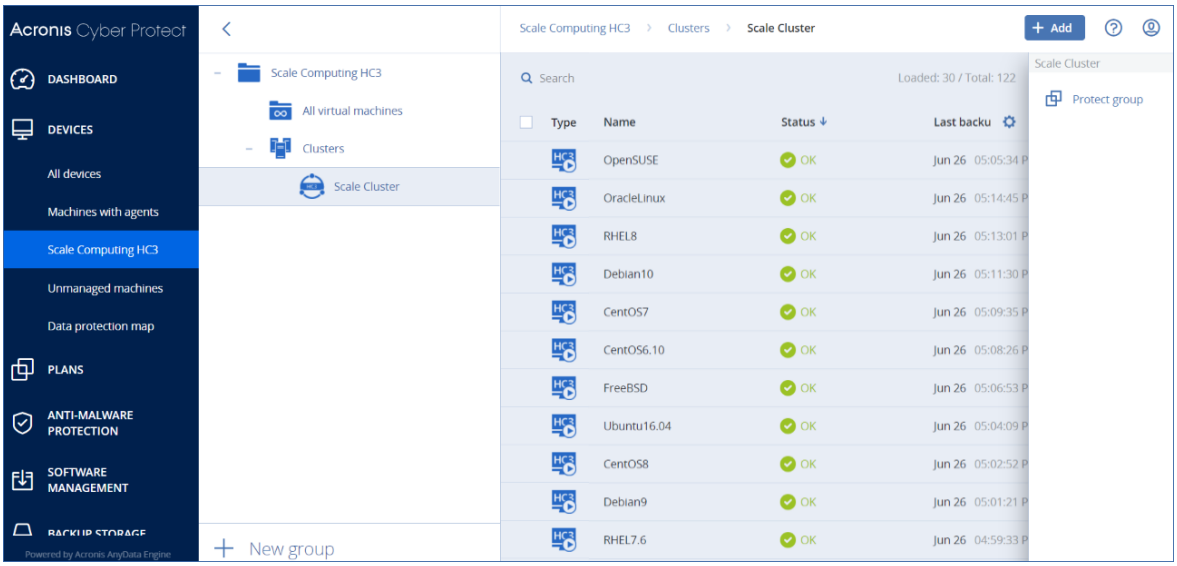
6. [Opcjonalnie] Podaj nazwę agenta. Nazwa będzie wyświetlana w konsoli internetowej Cyber Protect.



7. [Opcjonalnie] Wybierz strefę czasową swojej lokalizacji, aby mieć pewność, że zaplanowane operacje zostaną uruchomione w odpowiednim czasie.

Aby chronić maszyny wirtualne w klastrze Scale Computing HC3

1. Zaloguj się na koncie Cyber Protect.
2. Przejdź do sekcji **Urządzenia** > **Scale Computing HC3** > <klaster> lub znajdź komputery w sekcji **Urządzenia** > **Wszystkie urządzenia**.
3. Wybierz odpowiednie maszyny i zastosuj do nich plan ochrony.



Agent dla Scale Computing HC3 (urządzenie wirtualne) — wymagane role

W tej sekcji opisano role wymagane do wykonywania operacji z udziałem maszyn wirtualnych Scale Computing HC3, a także do wdrażania urządzeń wirtualnych.

Operacja	Rola
Tworzenie kopii zapasowych maszyn wirtualnych	Kopia zapasowa Tworzenie/edycja maszyn wirtualnych Usuwanie maszyn wirtualnych
Odzyskiwanie na istniejącą maszynę wirtualną	Kopia zapasowa Tworzenie/edycja maszyn wirtualnych Kontrola włączenia maszyn wirtualnych Usuwanie maszyn wirtualnych Ustawienia klastra
Odzyskiwanie danych na nową maszynę wirtualną	Kopia zapasowa Tworzenie/edycja maszyn wirtualnych Kontrola włączenia maszyn wirtualnych Usuwanie maszyn wirtualnych Ustawienia klastra
Wdrożenia urządzenia wirtualnego	Tworzenie/edycja maszyn wirtualnych

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 internetowej Cyber Protect.

Krok 1: Generowanie tokenu rejestracji

Token rejestracji przekazuje programowi instalacyjnemu dane o tożsamości użytkownika bez zapisywania nazwy logowania i hasła do konsoli internetowej Cyber Protect. Umożliwia to rejestrację na koncie dowolnej liczby maszyn. Aby ta operacja była bezpieczniejsza, token ma ograniczony okres ważności.

Aby wygenerować token rejestracji

1. Zaloguj się do konsoli internetowej Cyber Protect przy użyciu poświadczeń konta, do którego mają zostać przypisane komputery.
2. Kliknij **Wszystkie urządzenia** > **Dodaj**.
3. Przewiń w dół do pozycji **Token rejestracji** i kliknij **Wygeneruj**.
4. Określ okres ważności tokenu, a następnie kliknij **Wygeneruj token**.
5. Skopiuj lub zapisz token. Jeśli będziesz jeszcze potrzebować tokenu, koniecznie go zapisz. Możesz kliknąć **Zarządzaj aktywnymi tokenami**, aby wyświetlić już wygenerowane tokeny i nimi zarządzać. Uwaga: ze względów bezpieczeństwa w tabeli nie są pokazywane pełne wartości tokenów.

Krok 2: 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. Uruchom program instalacyjny.
4. Kliknij **Utwórz pliki .mst i .msi na potrzeby instalacji nienadzorowanej**.
5. Przejrzyj lub zmodyfikuj ustawienia instalacji, które zostaną dodane do pliku .mst. Wskazując metodę nawiązania połączenia z serwerem zarządzania, wybierz **Użyj tokenu rejestracji**, a następnie wprowadź wygenerowany token.
6. Kliknij **Kontynuuj**.
7. W oknie **Zapisz pliki w** określ ścieżkę utworzonego folderu.
8. Kliknij **Wygeneruj**.

W wyniku tego zostanie wygenerowana transformacja .mst, a do utworzonego folderu zostaną wyodrębnione pakiety instalacyjne .msi oraz .cab.

Krok 3: 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 systemie Windows Server 2008 lub nowszym).
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 systemie Windows Server 2008 lub nowszym:
   - 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 systemie Windows Server 2008 lub nowszym w obszarze **Obiekty zasad grupy** kliknij prawym przyciskiem myszy obiekt Zasady 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 lub nowszym:
   - Rozwiń węzły **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**.

Aktualizacja urządzeń wirtualnych

Wdrożenia lokalne

Aby zaktualizować agenta dla urządzenia wirtualnego (agent dla VMware lub agent dla Scale Computing HC3) w wersji starszej niż 15.24426 (wydanej we wrześniu 2020 r.), postępuj zgodnie z procedurą w "Aktualizowanie agentów" (s. 186).

Aby zaktualizować urządzenie wirtualne w wersji 15.24426 lub nowszej:

1. Pobierz pakiet aktualizacji, tak jak opisano w http://kb.acronis.com/latest.
2. Zapisz pliki `tar.bz` w następującym katalogu na komputerze serwera zarządzania:
   - Windows: `C:\Program Files\Acronis\VirtualAppliances\va-updates`
   - Linux: `/usr/lib/Acronis/VirtualAppliances/va-updates`
3. W konsoli internetowej Cyber Protect kliknij **Ustawienia** > **Agenci**.

   W oprogramowaniu zostanie wyświetlona lista komputerów. Komputery z nieaktualnymi wersjami urządzeń wirtualnych są oznaczone pomarańczowym wykrzyknikiem.
4. Wybierz komputery, na których chcesz zaktualizować urządzenia wirtualne. Komputery muszą być w trybie online.
5. Kliknij **Aktualizuj agenta**.
6. Wybierz agenta wdrażania.
7. Określ poświadczenia dostępu do konta z uprawnieniami administracyjnymi na komputerze docelowym.
8. Wybierz nazwę lub adres IP, których agent będzie używać w celu uzyskania dostępu do serwera zarządzania.

   Nazwa serwera jest domyślnie wybrana. Jeśli serwer DNS nie może przypisać nazwy hosta do adresu IP, co skutkuje błędem w trakcie rejestracji urządzenia wirtualnego, trzeba zmienić to ustawienie.

Postęp aktualizacji będzie widoczny na karcie **Działania**.

Uwaga
Podczas aktualizacji wszelkie trwające operacje tworzenia kopii zapasowych zakończą się niepowodzeniem.

Wdrożenie chmurowe

Informacje na temat aktualizacji urządzenia wirtualnego w chmurze można znaleźć w dokumentacji Aktualizowanie agentów w chmurze.

Aktualizowanie agentów

Wymagania wstępne

Na komputerach z systemem Windows funkcje usługi Cyber Protect wymagają pakietu redystrybucyjnego Microsoft Visual C++ 2017. Sprawdź, czy jest on już zainstalowany na komputerze, i ewentualnie zainstaluj go przed zaktualizowaniem agenta. Po zainstalowaniu pakietu może być wymagane ponowne uruchomienie komputera. Pakiet redystrybucyjny Microsoft Visual C++ można znaleźć tutaj: https://support.microsoft.com/help/2999226/update-for-universal-c-runtime-in-windows.

Aby sprawdzić wersję agenta, wybierz komputer, a następnie kliknij **Szczegóły**.

Możesz zaktualizować agenty przy użyciu konsoli internetowej Cyber Protect, ponawiając ich instalację w dowolny dostępny sposób. Aby zaktualizować wiele agentów naraz, skorzystaj z poniższej procedury.

Aby zaktualizować agenty przy użyciu konsoli internetowej Cyber Protect

1. [Tylko w przypadku wdrożenia lokalnego] Zaktualizuj serwer zarządzania.
2. [Tylko w przypadku wdrożenia lokalnego] Upewnij się, że pakiety instalacyjne znajdują się na komputerze z serwerem zarządzania. Dokładne instrukcje można znaleźć w sekcji „Dodawanie komputera z systemem Windows” > „Pakiety instalacyjne”.
3. W konsoli internetowej Cyber Protect kliknij **Ustawienia** > **Agenci**.
   W oprogramowaniu zostanie wyświetlona lista komputerów. Komputery z nieaktualnymi wersjami agentów są oznaczone pomarańczowym wykrzyknikiem.
4. Wybierz komputery, na których chcesz zaktualizować agenty. Komputery te muszą być w trybie online.
5. Kliknij **Aktualizuj agenta**.
6. Wybierz agenta wdrażania.
7. Określ poświadczenia dostępu do konta z uprawnieniami administracyjnymi na komputerze docelowym.
8. Wybierz nazwę lub adres IP serwera zarządzania, których agent będzie używać w celu uzyskania dostępu do tego serwera.
   Domyślnie wybrana jest nazwa serwera. Jeśli serwer zarządzania ma więcej niż jeden interfejs sieciowy lub występują problemy z usługą DNS, które powodują niepowodzenie rejestracji agenta, może być konieczne wybranie adresu IP.
9. [Tylko w przypadku wdrożeń lokalnych] Postęp aktualizacji będzie widoczny na karcie **Działania**.

Uwaga
Podczas aktualizacji wszelkie trwające operacje tworzenia kopii zapasowych zakończą się niepowodzeniem.

Aby zaktualizować definicje usługi Cyber Protect na komputerze

1. Kliknij **Ustawienia** > **Agenty**.
2. Wybierz komputer, na którym chcesz zaktualizować definicje usługi Cyber Protect, i kliknij **Aktualizuj definicje**. Komputery te muszą być w trybie online.

Aby przypisać rolę aktualizatora do agenta

1. Kliknij **Ustawienia** > **Agenty**.
2. Wybierz komputer, do którego chcesz przypisać rolę aktualizatora, kliknij **Szczegóły**, a następnie w sekcji **Definicje usługi Cyber Protect** włącz opcję **Użyj tego agenta, aby pobrać oraz rozpowszechnić poprawki i aktualizacje**.

Aby wyczyścić dane z pamięci podręcznej agenta

1. Kliknij **Ustawienia** > **Agenty**.
2. Wybierz komputer, na którym chcesz wyczyścić dane z pamięci podręcznej (przestarzałe pliki aktualizacji i dane zarządzania poprawkami), i kliknij **Wyczyść pamięć podręczną**.

Uaktualnienie do rozwiązania Acronis Cyber Protect 15

Starszą wersję produktu można uaktualnić do rozwiązania Acronis Cyber Protect 15 następująco:

- Bezpośrednio, bez odinstalowywania starszej wersji produktu.
  Ta możliwość jest dostępna tylko w przypadku produktu Acronis Backup 12.5 Update 5 (kompilacja 16180) lub nowszego.
- Przez odinstalowanie starszej wersji produktu i zainstalowanie od nowa rozwiązania Acronis Cyber Protect 15.
  Ta możliwość jest dostępna w przypadku wszystkich kwalifikujących się produktów. Dodatkowe informacje o tych produktach można znaleźć w tym artykule bazy wiedzy Knowledge Base.

Uwaga
Zaleca się utworzenie kopii zapasowej systemu przed uaktualnieniem. W razie niepowodzenia uaktualnienia pozwoli ona wrócić do oryginalnej konfiguracji.

Aby rozpocząć uaktualnianie, uruchom instalator i wykonuj instrukcje wyświetlane na ekranie.

Serwer zarządzania w programie Acronis Cyber Protect 15 jest kompatybilny wstecz i obsługuje agenty z wersji 12.5. Agenty te jednak nie obsługują funkcji programu Cyber Protect.

Uaktualnienie agentów nie powoduje żadnych zakłóceń dotyczących istniejącego zestawu kopii zapasowych ani ich ustawień.

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 **Do pobrania** (kliknij ikonę konta widoczną w prawym górnym rogu > **Do pobrania**).

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

Ostrzeżenie!
W przypadku wdrożeń lokalnych należy zachować wyjątkową ostrożność przy wybieraniu komponentów do deinstalacji.

W przypadku przypadkowej deinstalacji serwera zarządzania konsola internetowa Cyber Protect nie będzie dostępna, nie będzie można utworzyć kopii zapasowej ani odzyskać żadnego z komputerów zarejestrowanych na odinstalowanym 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 Cyber Protect** > **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 internetowej Cyber Protect, a kopie zapasowe starego komputera nie zostaną powiązane z nowym komputerem.
4. Potwierdź decyzję.

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 internetowej Cyber Protect, a kopie zapasowe starego komputera nie zostaną powiązane z nowym komputerem.
3. Potwierdź decyzję.

W systemie macOS

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.

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.
3. Jeśli urządzenie wirtualne używa magazynu dołączonego lokalnie na dysku wirtualnym i chcesz zachować dane na tym dysku, wykonaj następujące czynności:
   a. Kliknij urządzenie wirtualne prawym przyciskiem myszy, 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 podłączyć do innego urządzenia wirtualnego.
4. Kliknij urządzenie wirtualne prawym przyciskiem myszy, a następnie kliknij **Usuń z dysku**. Potwierdź decyzję.

Usuwanie komputerów z konsoli internetowej Cyber Protect

Po odinstalowaniu agenta zostanie on wyrejestrowany z serwera zarządzania, a komputer, na którym agent został zainstalowany, zostanie automatycznie usunięty z konsoli internetowej Cyber Protect.

Jeśli jednak w trakcie tej operacji połączenie z serwerem zarządzania zostanie utracone, na przykład z powodu problemu z siecią, może się zdarzyć, że agent zostanie odinstalowany, a jego komputer nadal będzie widoczny w konsoli internetowej. W takim przypadku należy ręcznie usunąć ten komputer z konsoli internetowej.

Aby ręcznie usunąć komputer z konsoli internetowej:

1. W konsoli internetowej Cyber Protect przejdź do sekcji **Ustawienia** > **Agenci**.
2. Wybierz komputer, na którym został zainstalowany agent.
3. Kliknij **Usuń**.

Dostęp do konsoli internetowej Cyber Protect

Aby uzyskać dostęp do konsoli internetowej Cyber Protect, wprowadź adres strony logowania w pasku adresu przeglądarki internetowej, a następnie zaloguj się w niżej opisany sposób.

Wdrożenie lokalne

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

Oba protokoły — HTTP i HTTPS — są obsługiwane przez ten sam port TCP, który można skonfigurować podczas instalacji serwera zarządzania. Portem domyślnym jest port 9877.

Serwer zarządzania można skonfigurować tak, aby blokował dostęp do konsoli internetowej Cyber Protect przy użyciu protokołu HTTP i używał certyfikatu SSL innej firmy.

W systemie Windows

Jeśli serwer zarządzania jest zainstalowany w systemie Windows, istnieją dwa sposoby zalogowania się do konsoli internetowej Cyber Protect:

- Kliknij **Zaloguj się**, aby się zalogować jako bieżący użytkownik systemu Windows.
  To jest najłatwiejszy sposób zalogowania się z tego samego komputera, na którym jest zainstalowany serwer zarządzania.
  Jeśli serwer zarządzania jest zainstalowany na innym komputerze, ta metoda działa, pod warunkiem, że:
  - Komputer, z którego się logujesz, znajduje się w tej samej domenie usługi Active Directory co serwer zarządzania.
  - Logujesz się jako zwykły użytkownik domeny.

  Zalecamy skonfigurowanie przeglądarki internetowej dla zintegrowanego uwierzytelniania systemu Windows. W przeciwnym razie przeglądarka zapyta o nazwę użytkownika i hasło. Możesz jednak tę opcję wyłączyć.
- Kliknij **Wprowadź nazwę użytkownika i hasło**, a następnie podaj nazwę użytkownika i hasło.

W każdym przypadku Twoje konto musi znajdować się na liście administratorów serwera zarządzania. Domyślnie ta lista zawiera grupę **Administratorzy** na komputerze z uruchomionym serwerem zarządzania. Aby uzyskać więcej informacji, zobacz „Administratorzy i jednostki”.

Aby wyłączyć opcję Zaloguj się, aby się zalogować jako bieżący użytkownik systemu Windows

1. Na komputerze, na którym jest zainstalowany serwer zarządzania, przejdź do folderu `C:\Program Files\Acronis\AccountServer`.
2. Otwórz do edycji plik **account_server.json**.
3. Przejdź do sekcji „connectors” (łączniki) i usuń następujące wiersze:

```
{
"type": "sspi",
"name": "1 Windows Integrated Logon",
"id": "sspi",
"config": {}
},
```

4. Przejdź do sekcji „checksum” (suma kontrolna) i zmień wartość „sum” następująco:

```
"sum": "FWY/8e8C6c0AgNl0BfCrjgT4v2uj7RQNmaIYbwbjpzU="
```

5. Uruchom ponownie usługę Acronis Service Manager Service zgodnie z opisem zamieszczonym w sekcji „Stosowanie certyfikatu wydanego przez zaufany podmiot certyfikujący”.

W systemie Linux

Jeśli serwer zarządzania został zainstalowany w systemie Linux, określ nazwę użytkownika i hasło konta znajdującego się na liście administratorów serwera zarządzania. Domyślnie lista ta zawiera tylko użytkownika **root** komputera z serwerem zarządzania. Aby uzyskać więcej informacji, zobacz „Administratorzy i jednostki”.

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 konta w prawym górnym rogu.

Konfigurowanie przeglądarki internetowej dla zintegrowanego uwierzytelniania systemu Windows

Zintegrowane uwierzytelnianie systemu Windows jest możliwe, jeśli konsola internetowa Cyber Protect zostanie otwarta z komputera z systemem Windows i dowolną obsługiwaną przeglądarką.

Zalecamy skonfigurowanie przeglądarki internetowej dla zintegrowanego uwierzytelniania systemu Windows. W przeciwnym razie przeglądarka zapyta o nazwę użytkownika i hasło.

Konfigurowanie przeglądarki Internet Explorer, Microsoft Edge, Opera i Google Chrome

Jeśli komputer, na którym działa przeglądarka, znajduje się w tej samej domenie usługi Active Directory, co komputer, na którym działa serwer zarządzania, dodaj stronę logowania konsoli do listy witryn **Lokalny intranet**.

W przeciwnym razie dodaj stronę logowania konsoli do listy **Zaufane witryny** i włącz ustawienie **Automatyczne logowanie za pomocą bieżącej nazwy użytkownika i hasła**.

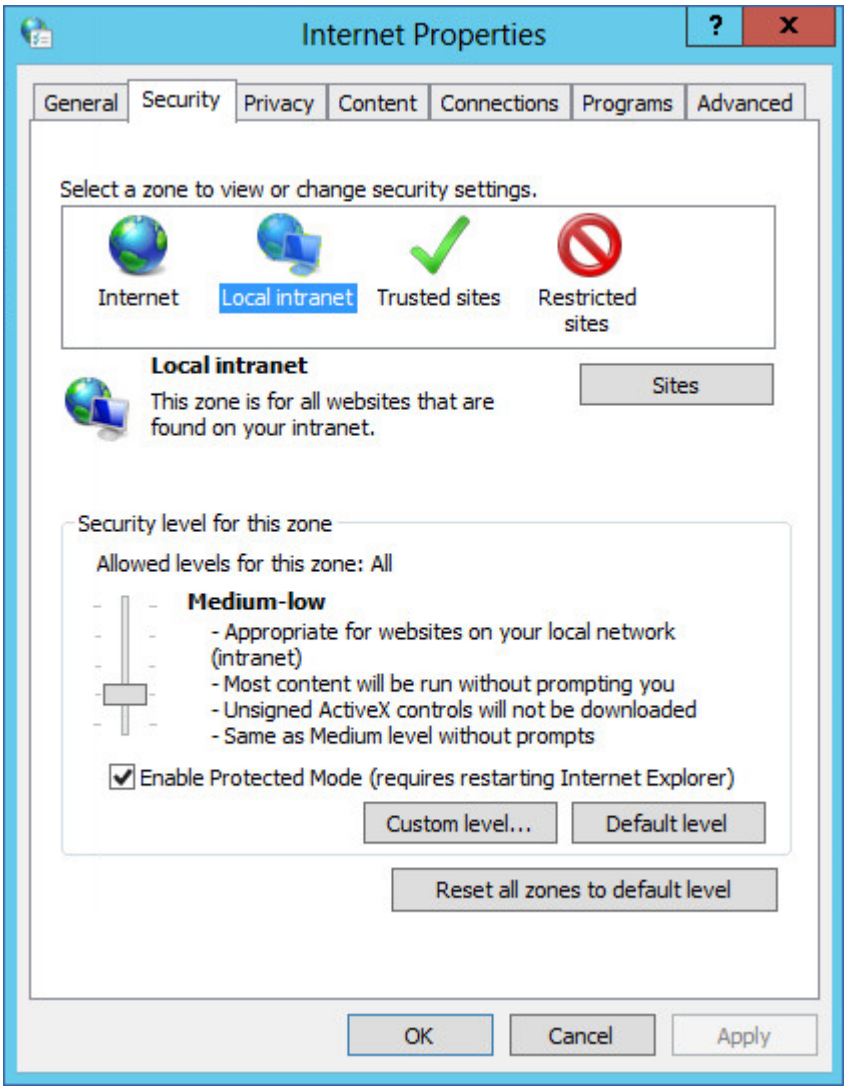
Szczegółowe instrukcje znajdują się w dalszej części tej sekcji. Ponieważ te przeglądarki używają ustawień systemu Windows, można je również skonfigurować przy użyciu zasad grupy w domenie Active Directory.

Konfigurowanie przeglądarki Mozilla Firefox

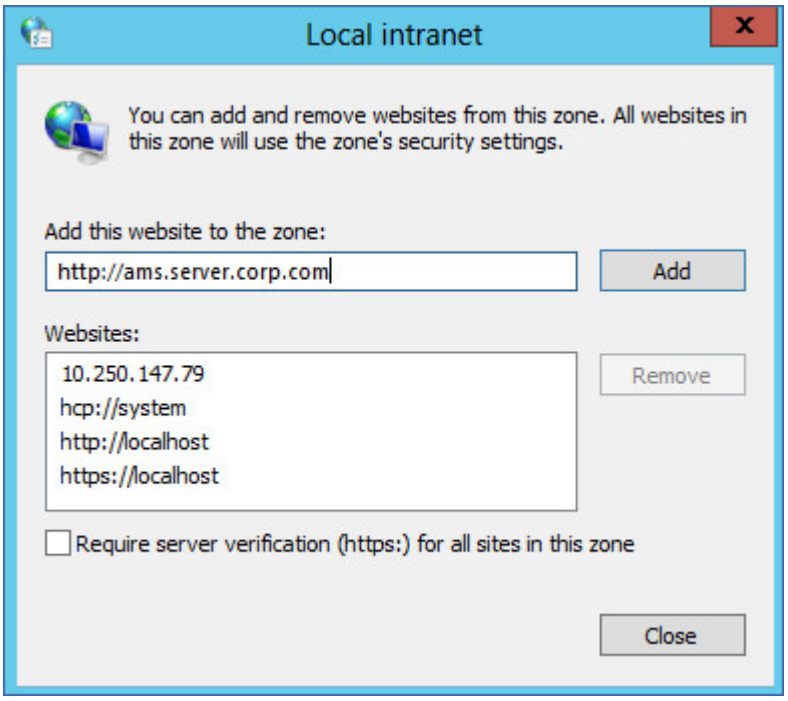
1. W programie Firefox przejdź do adresu URL `about:config`, a następnie kliknij **Akceptuję ryzyko**.
2. W polu **Wyszukiwanie** znajdź preferencję `network.negotiate-auth.trusted-uris`.
3. Kliknij dwukrotnie tę preferencję, a następnie wprowadź adres strony logowania do konsoli internetowej Cyber Protect.
4. Powtórz kroki 2-3 dla preferencji `network.automatic-ntlm-auth.trusted-uris`.
5. Zamknij okno `about:config`.

Dodawanie konsoli do listy lokalnych stron intranetowych

1. Przejdź do **Panel sterowania** > **Opcje internetowe**.
2. Na karcie **Zabezpieczenia** wybierz **Lokalny intranet**.



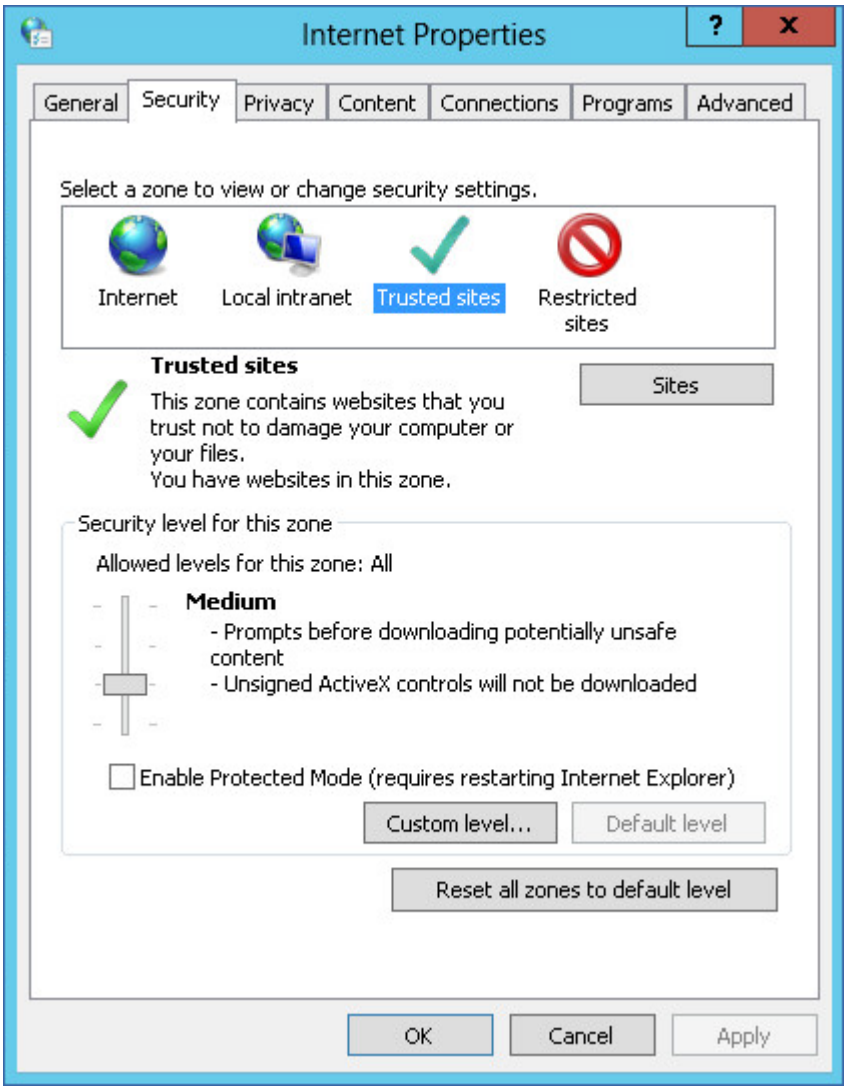
3. Kliknij **Witryny**.
4. W polu **Dodaj tę witrynę internetową do strefy** wprowadź adres strony logowania do konsoli internetowej Cyber Protect, a następnie kliknij **Dodaj**.



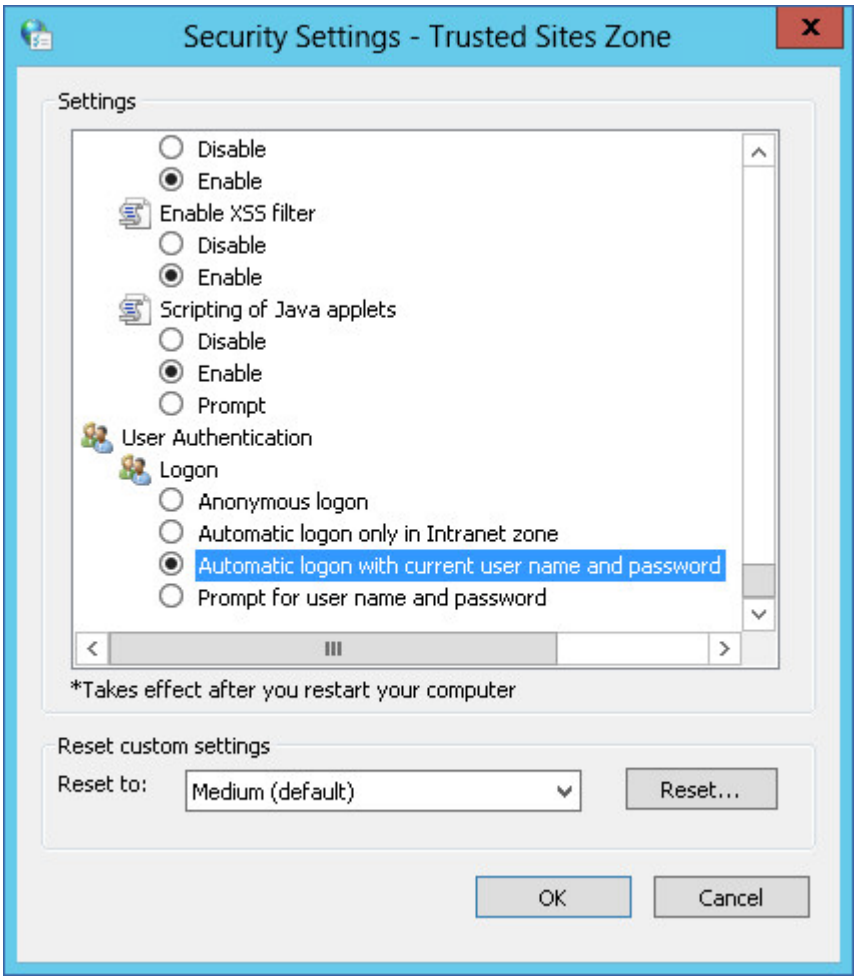
5. Kliknij **Zamknij**.
6. Kliknij **OK**.

Dodawanie konsoli do listy witryn zaufanych

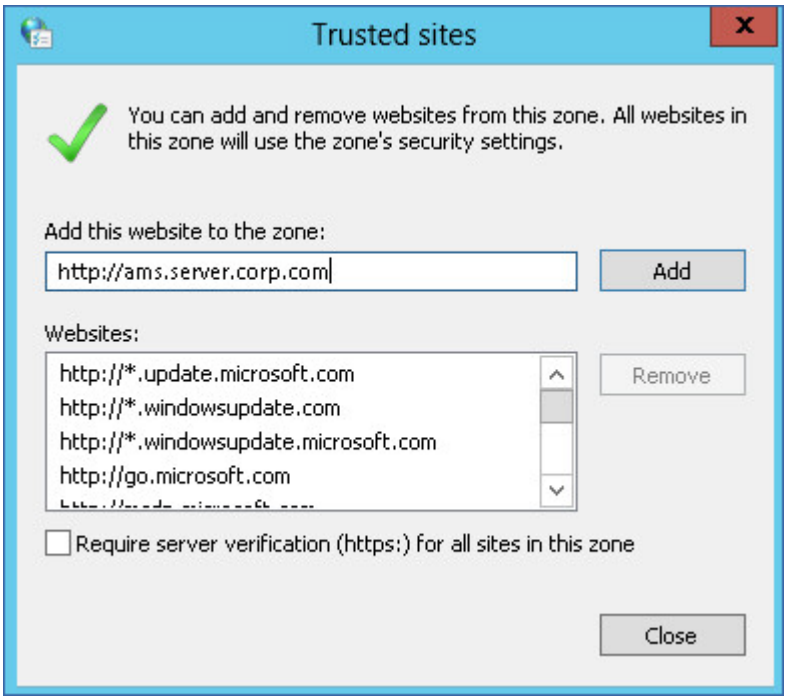
1. Przejdź do **Panel sterowania** > **Opcje internetowe**.
2. Na karcie **Zabezpieczenia** wybierz **Zaufane witryny**, a następnie kliknij **Poziom niestandardowy**.



3. W obszarze **Logowanie** wybierz **Automatyczne logowanie za pomocą bieżącej nazwy użytkownika i hasła**, a następnie kliknij **OK**.



4. Na karcie **Zabezpieczenia**, mając nadal wybrane **Zaufane witryny**, kliknij **Witryny**.
5. W polu **Dodaj tę witrynę internetową do strefy** wprowadź adres strony logowania do konsoli internetowej Cyber Protect, a następnie kliknij **Dodaj**.



6. Kliknij **Zamknij**.
7. Kliknij **OK**.

Zezwalanie na łączenie się z konsolą internetową tylko przy użyciu protokołu HTTPS

Ze względów bezpieczeństwa można uniemożliwić użytkownikom uzyskiwanie dostępu do konsoli internetowej Cyber Protect przy użyciu protokołu HTTP i zezwolić tylko na połączenia HTTPS.

Aby zezwolić łączenie się z konsolą internetową tylko przy użyciu protokołu HTTPS

1. Na komputerze z uruchomionym serwerem zarządzania otwórz za pomocą edytora tekstowego następujący plik konfiguracyjny:
   - W systemie Windows: `%ProgramData%\Acronis\ApiGateway\api_gateway.json`
   - W systemie Linux: `/var/lib/Acronis/ApiGateway/api_gateway.json`
2. Odszukaj następującą sekcję:

   ```
   "tls": {
     "auto_redirect" : false,
     "cert_file": "cert.pem",
   ```

3. Zmień wartość parametru `"auto_redirect"` z `false` na `true`.
   Jeśli nie ma wiersza `"auto_redirect"`, dodaj go ręcznie:

   ```
   "auto_redirect": true,
   ```

4. Zapisz plik `api_gateway.json`.

Ważne
Zachowaj ostrożność i postaraj się nie usunąć przypadkowo żadnych przecinków, nawiasów ani cudzysłowów w pliku konfiguracyjnym.

5. Uruchom ponownie usługę Acronis Service Manager Service zgodnie z poniższym opisem.

Aby uruchomić ponownie usługę Acronis Service Manager Service w systemie Windows

W systemie Windows

1. W menu **Start** kliknij **Uruchom**, a następnie wpisz: **cmd**.
2. Kliknij **OK**.
3. Uruchom następujące polecenia:

```
net stop asm
net start asm
```

W systemie Linux

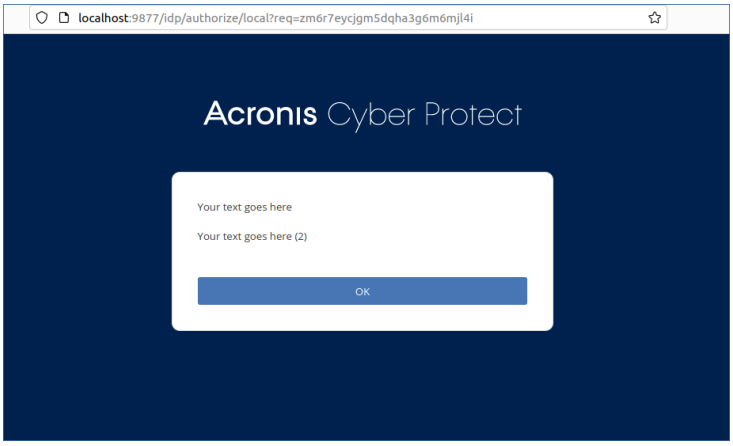
1. Otwórz **Terminal**.
2. W dowolnym katalogu uruchom następujące polecenie:

```
sudo service acronis_asm restart
```

Dodawanie własnego komunikatu do konsoli internetowej

Do konsoli internetowej Cyber Protect można dodać własny komunikat.

Komunikat ten będzie wyświetlany przed każdą próbą zalogowania się.



Wymagania wstępne

Jeśli do komputera, na którym działa serwer zarządzania, zastosowano jakiekolwiek plany ochrony, należy się upewnić, że funkcja ochrony własnej jest wyłączona. W przeciwnym razie nie będzie można edytować pliku konfiguracyjnego.

Dodatkowe informacje o tym, jak wyłączyć lub włączyć funkcję ochrony własnej, można znaleźć w sekcji "Ochrona własna" (s. 532).

Aby dodać własny komunikat do konsoli internetowej

W systemie Windows

1. Zaloguj się na komputerze z zainstalowanym serwerem zarządzania. Twoje konto musi mieć prawa administratora.
2. Przejdź do folderu `%Program Files%\Acronis\AccountServer`.
3. [Opcjonalnie] Utwórz kopię zapasową pliku `AccountServer.zip`.
4. Przejdź do folderu `%Program Files%\Acronis\AccountServer\AccountServer.zip\static\locale`.
5. Rozpakuj plik JSON odpowiadający językowi używanemu w konsoli internetowej Cyber Protect. Jeśli na przykład używasz języka angielskiego, rozpakuj plik `en.json`.

   Uwaga
   Aby edytować plik, trzeba go rozpakować, a nie tylko otworzyć przez dwukrotne kliknięcie.

6. Otwórz rozpakowany plik do edycji. Możesz użyć edytora tekstowego, na przykład programu Notatnik lub Notepad++.
7. Przejdź do następującego wiersza i dodaj przecinek na końcu:

   ```
   "APP_LOGINFORM_LOGIN_BUTTON": "Log in",
   ```

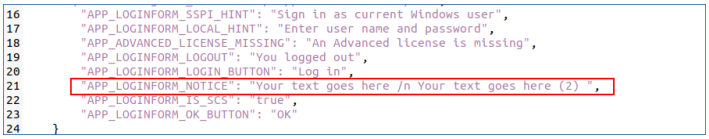
8. Pod wierszem `"APP_LOGINFORM_LOGIN_BUTTON": "Log in"` dodaj następujące wiersze:

   ```
   "APP_LOGINFORM_NOTICE": "<Type your custom message here>",
   ```

   ```
   "APP_LOGINFORM_IS_SCS": "true",
   ```

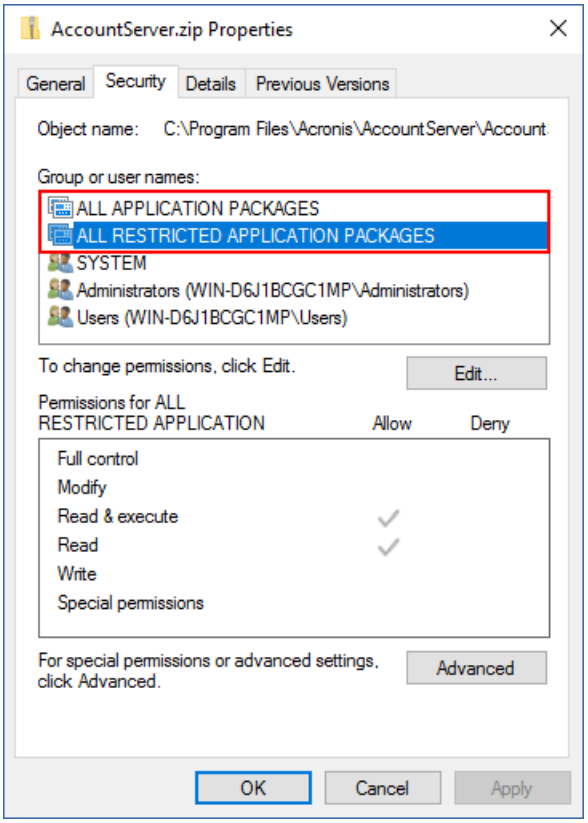
   ```
   "APP_LOGINFORM_OK_BUTTON": "OK"
   ```

   Na przykład:

9. Zapisz zmiany, a następnie umieść edytowany plik JSON z powrotem w folderze `%Program Files%\Acronis\AccountServer\AccountServer.zip\static\locale`.

10. Kliknij prawym przyciskiem myszy plik `AccountServer.zip`, a następnie przejdź do sekcji **Właściwości** > **Zabezpieczenia**, aby sprawdzić, czy `WSZYSTKIE PAKIETY APLIKACJI` i `WSZYSTKIE PAKIETY APLIKACJI Z OGRANICZENIAMI` dodano w obszarze **Grupa lub nazwy użytkowników** z prawami **Odczyt** oraz **Odczyt i wykonanie**.



Uwaga

Jeśli brakuje pozycji `WSZYSTKIE PAKIETY APLIKACJI Z OGRANICZENIAMI`, usuń pozycję `WSZYSTKIE PAKIETY APLIKACJI` z listy, a następnie dodaj ją ponownie. Pozycja `WSZYSTKIE PAKIETY APLIKACJI Z OGRANICZENIAMI` pojawi się automatycznie po dodaniu pozycji `WSZYSTKIE PAKIETY APLIKACJI`.

11. Uruchom ponownie usługę **Acronis Service Manager Service** zgodnie z opisem podanym w sekcji "Aby uruchomić ponownie usługę Acronis Service Manager Service" (s. 204).

W systemie Linux

1. Zaloguj się na komputerze z zainstalowanym serwerem zarządzania.
2. Przejdź do folderu `/usr/lib/Acronis/AccountServer`.
3. Upewnij się, że masz uprawnienia do zapisu w przypadku pliku `AccountServer.zip`.
4. [Opcjonalnie] Utwórz kopię zapasową pliku `AccountServer.zip`.
5. Przejdź do folderu `/usr/lib/Acronis/AccountServer/static/locale`.
6. Rozpakuj plik JSON odpowiadający językowi używanemu w konsoli internetowej Cyber Protect. Jeśli na przykład używasz języka angielskiego, rozpakuj plik `en.json`.
7. Otwórz rozpakowany plik do edycji.

8. Przejdź do następującego wiersza i dodaj przecinek na końcu:

```
"APP_LOGINFORM_LOGIN_BUTTON": "Log in",
```

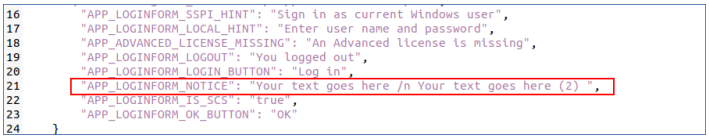
9. Pod wierszem `"APP_LOGINFORM_LOGIN_BUTTON": "Log in"` dodaj następujące wiersze:

```
"APP_LOGINFORM_NOTICE": "<Type your custom message here>",
```

```
"APP_LOGINFORM_IS_SCS": "true",
```

```
"APP_LOGINFORM_OK_BUTTON": "OK"
```

Na przykład:



10. Zapisz zmiany, a następnie umieść edytowany plik JSON z powrotem w folderze `/usr/lib/Acronis/AccountServer/static/locale`.
11. Uruchom ponownie usługę **Acronis Service Manager Service** zgodnie z opisem podanym w sekcji "Aby uruchomić ponownie usługę Acronis Service Manager Service" (s. 204).

Ustawienia certyfikatów SSL

W tej sekcji opisano, jak:

- Skonfigurować agenta ochrony, który używa certyfikatu Secure Socket Layer (SSL) z podpisem własnym wygenerowanego przez serwer zarządzania.
- Wymienić certyfikat SSL z podpisem własnym wygenerowany przez serwer zarządzania na certyfikat wystawiony przez zaufany podmiot certyfikujący, taki jak GoDaddy, Comodo czy GlobalSign. Jeśli to zrobisz, certyfikat używany przez serwer zarządzania będzie certyfikatem zaufanym na każdym komputerze. W przypadku logowania się do konsoli internetowej Cyber Protect przy użyciu protokołu HTTPS nie będzie wyświetlany alert bezpieczeństwa przeglądarki.

Opcjonalnie można skonfigurować serwer zarządzania tak, aby blokował dostęp do konsoli internetowej Cyber Protect przy użyciu protokołu HTTP przez przekierowywanie wszystkich użytkowników do strony HTTPS.

Stosowanie certyfikatu z podpisem własnym

Aby skonfigurować agenta ochrony w systemie Windows

1. Na komputerze z agentem otwórz Edytor rejestru.
2. Odszukaj następujący klucz rejestru: **HKEY_LOCAL_MACHINE\Software\Acronis\BackupAndRecovery\Settings\CurlOptions.**
3. Ustaw wartość **VerifyPeer** na **0**.

4. Dopilnuj, aby wartość **VerifyHost** była ustawiona na **0**.
5. Uruchom ponownie usługę Managed Machine Service (MMS):
   a. W menu **Start** kliknij **Uruchom**, a następnie wpisz: **cmd**.
   b. Kliknij **OK**.
   c. Uruchom następujące polecenia:

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

Aby skonfigurować agenta ochrony w systemie Linux

1. Na komputerze z agentem otwórz do edycji plik **/etc/Acronis/BackupAndRecovery.config.**
2. Przejdź do klucza **CurlOptions** i ustaw wartość **VerifyPeer** na **0.** Dopilnuj, aby wartość **VerifyHost** również była ustawiona na **0**.
3. Zapisz zmiany.
4. Uruchom ponownie usługę Managed Machine Service (MMS), wykonując w dowolnym katalogu następujące polecenie:

```
sudo service acronis_mms restart
```

Aby skonfigurować agenta ochrony w systemie macOS

1. Na komputerze z agentem zatrzymaj usługę Managed Machine Service (MMS):
   a. Przejdź do sekcji **Aplikacje** > **Narzędzia** > **Terminal**.
   b. Uruchom następujące polecenie:

```
sudo launchctl stop acronis_mms
```

2. Otwórz do edycji plik **/Library/Application Support/Acronis/Registry/BackupAndRecovery.config**.
3. Przejdź do klucza **CurlOptions** i ustaw wartość **VerifyPeer** na **0**. Dopilnuj, aby wartość **VerifyHost** również była ustawiona na **0**.
4. Zapisz zmiany.
5. Uruchom usługę Managed Machine Service (MMS), wykonując na terminalu następujące polecenie:

```
sudo launchctl starts acronis_mms
```

Stosowanie certyfikatu wydanego przez zaufany podmiot certyfikujący

Aby skonfigurować ustawienia certyfikatu SSL

1. Upewnij się, że masz wszystkie następujące elementy:

W przypadku korzystania z plików certyfikatu i klucza	W przypadku korzystania z pliku PFX
Plik certyfikatu (w formacie .pem)	Plik PFX
Plik z kluczem prywatnym certyfikatu (zwykle w formacie .key)	
Hasło do klucza prywatnego (jeśli klucz jest chroniony hasłem)	Hasło do pliku PFX, jeśli ten plik jest chroniony hasłem

2. Skopiuj plik na komputer z serwerem zarządzania.
3. Na tym komputerze otwórz w edytorze tekstowym następujący plik konfiguracyjny:
   - W systemie Windows: `%ProgramData%\Acronis\ApiGateway\api_gateway.json`
   - W systemie Linux: `/var/lib/Acronis/ApiGateway/api_gateway.json`
4. Odszukaj następującą sekcję:

```
"tls": {
    "cert_file": "cert.pem",
    "key_file": "key.pem",
    "passphrase": "",
```

5. W cudzysłowie w wierszu `"cert_file"` podaj pełną ścieżkę do pliku certyfikatu lub pliku PFX.
   Na przykład:

System operacyjny	W przypadku korzystania z połączenia certyfikatu i klucza	W przypadku korzystania z pliku .pfx
Windows (uwaga na ukośniki)	`"cert_file": "C:/certificate/local-domain.ams.pem"`	`"cert_file": "C:/certificate/local-domain.ams.pfx"`
Linux	`"cert_file": "/home/user/local-domain.ams.pem"`	`"cert_file": "/home/user/local-domain.ams.pfx"`

6. W cudzysłowie w wierszu `"key_file"` podaj pełną ścieżkę do pliku klucza prywatnego lub pliku PFX zawierającego klucz certyfikatu.
   Pik PFX zawiera zwykle zarówno certyfikat, jak i jego klucz. W takim przypadku w wierszu `"key_file"` podaj tę samą ścieżkę co w poprzednim kroku.
   Na przykład:

System operacyjny	W przypadku korzystania z połączenia certyfikatu i klucza	W przypadku korzystania z pliku .pfx
Windows	`"key_file":`	`"cert_file": "C:/certificate/local-`

System operacyjny	W przypadku korzystania z połączenia certyfikatu i klucza	W przypadku korzystania z pliku .pfx
(uwaga na ukośniki)	`"C:/certificate/private.key"`	`domain.ams.pfx"`
Linux	`"key_file": "/home/user/private.key"`	`"cert_file": "/home/user/local-domain.ams.pfx"`

7. [Opcjonalnie] Jeśli klucz prywatny lub plik PFX jest chroniony hasłem, w cudzysłowie w wierszu `"passphrase"` podaj odpowiednie hasło.

   Na przykład: `"passphrase": "moje hasło"`

   Uwaga
   Jeśli w pliku konfiguracyjnym `api_gateway.json` nie ma wiersza `"passphrase": ""`,, dodaj go ręcznie.

   Na przykład:

   ```
   "tls": {
       "cert_file": "cert.pem",
       "key_file": "key.pem",
       "passphrase": "my password",
   }
   ```

8. Zapisz plik `api_gateway.json`.

   Ważne
   Zachowaj ostrożność i postaraj się nie usunąć przypadkowo żadnych przecinków, nawiasów ani cudzysłowów w pliku konfiguracyjnym.

9. Uruchom ponownie usługę Acronis Service Manager Service zgodnie z poniższym opisem.

Aby uruchomić ponownie usługę Acronis Service Manager Service

W systemie Windows

1. W menu **Start** kliknij **Uruchom**, a następnie wpisz: **cmd**.
2. Kliknij **OK**.
3. Uruchom następujące polecenia:

   ```
   net stop asm
   net start asm
   ```

W systemie Linux

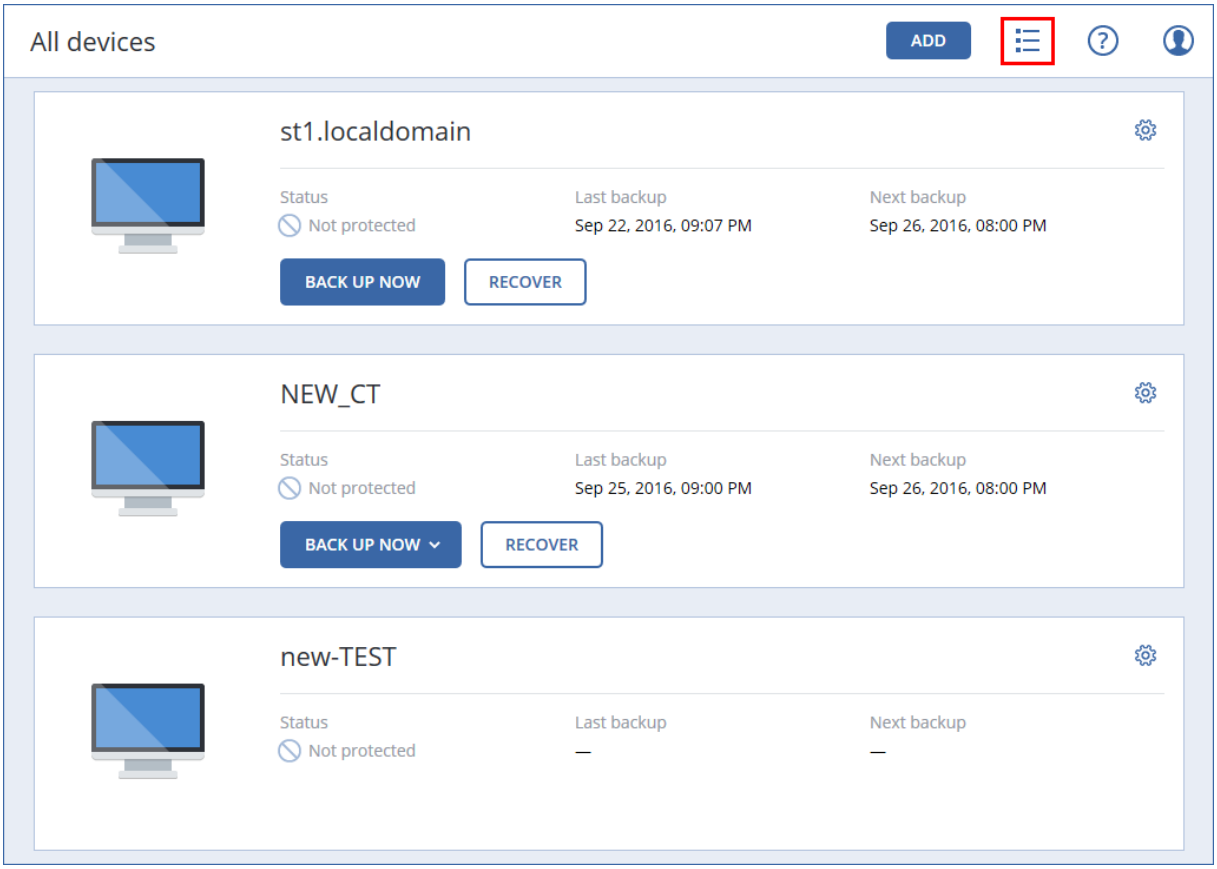
1. Otwórz **Terminal**.
2. W dowolnym katalogu uruchom następujące polecenie:

```
sudo service acronis_asm restart
```

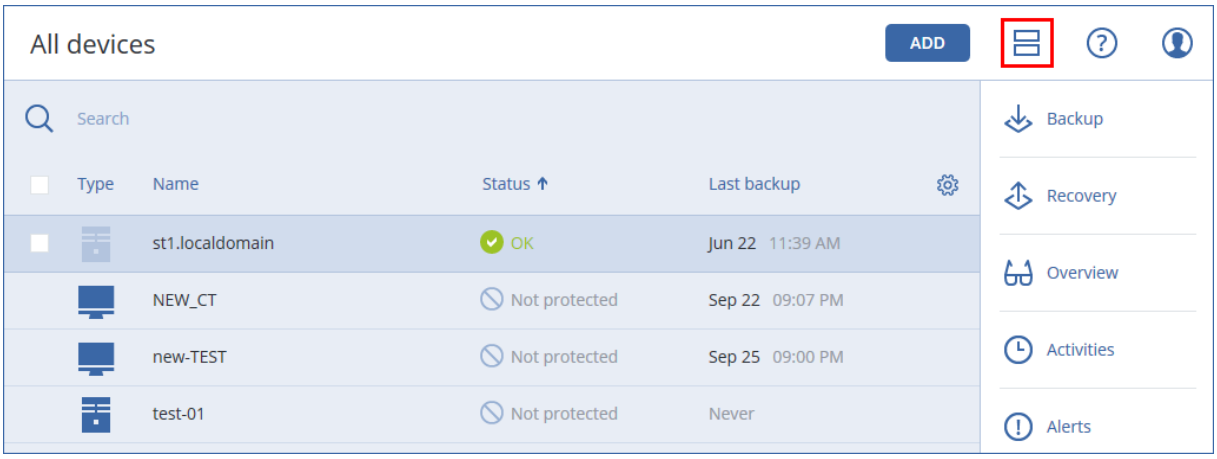
Widok konsoli internetowej Cyber Protect

W konsoli internetowej Cyber Protect są dostępne dwa widoki: widok prosty i widok tabeli. Aby przełączyć widok, kliknij odpowiednią ikonę w prawym górnym rogu.

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.

Kiedy komputer przejdzie w tryb online lub offline, trzeba trochę czasu, aby jego status w konsoli internetowej Cyber Protect uległ zmianie.

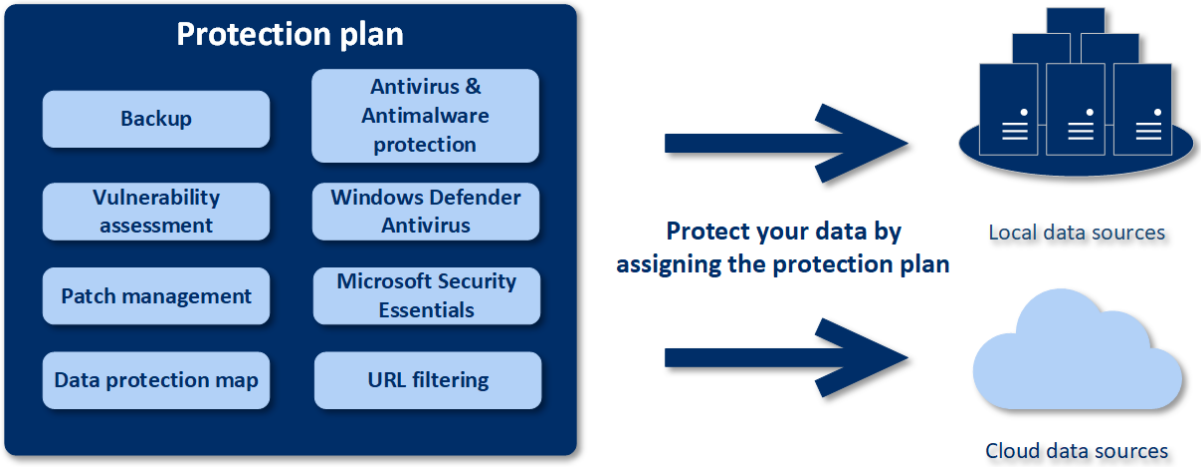
Status komputera jest sprawdzany co minutę. Jeśli agent zainstalowany na tym komputerze nie przesyła danych i brak odpowiedzi na pięć kolejnych operacji sprawdzania, komputer będzie wyświetlany jako offline. Komputer znów będzie wyświetlany jako online, gdy odpowie na zapytania sprawdzania statusu lub rozpocznie przesyłanie danych.

Plan ochrony i moduły

Plan ochrony to plan, który łączy w sobie kilka modułów ochrony danych, takich jak:

- Kopia zapasowa — umożliwia tworzenie kopii zapasowych źródeł danych na dysku lokalnym lub w chmurze.
- Ochrona przed wirusami i złośliwym oprogramowaniem — umożliwia sprawdzanie komputerów za pomocą wbudowanego rozwiązania antywirusowego.
- Filtrowanie adresów URL — umożliwia chronienie komputerów przed zagrożeniami pochodzącymi z Internetu przez blokowanie dostępu do złośliwych adresów URL i dostępnych do pobrania treści.
- Program antywirusowy Windows Defender — umożliwia zarządzanie ustawieniami programu antywirusowego Windows Defender w celu zapewnienia ochrony danego środowiska.
- Microsoft Security Essentials — umożliwia zarządzanie ustawieniami programu Microsoft Security Essentials w celu zapewnienia ochrony danego środowiska.
- Ocena luk w zabezpieczeniach — automatycznie sprawdza, czy w zabezpieczeniach produktów firmy Microsoft i innych firm zainstalowanych na komputerach nie ma luk, oraz powiadamia użytkownika o ich ewentualnym występowaniu.
- Zarządzanie poprawkami — umożliwia instalowanie na komputerach poprawek oraz aktualizacji do produktów firmy Microsoft i innych firm w celu wyeliminowania wykrytych luk w zabezpieczeniach.
- Mapa ochrony danych — umożliwia wykrywanie danych w celu monitorowania statusu ochrony ważnych plików.

Plan ochrony umożliwia pełną ochronę źródeł danych przed zagrożeniami zewnętrznymi i wewnętrznymi. Włączając i wyłączając różne moduły oraz konfigurując ich ustawienia, można tworzyć elastyczne plany zaspokajające różne potrzeby biznesowe.



Tworzenie planu ochrony

Plan ochrony można zastosować do wielu komputerów — w trakcie jego tworzenia lub później. Gdy tworzysz plan, system sprawdza system operacyjny i typ urządzenia (stacja robocza, maszyna wirtualna itp.) i wyświetla tylko te moduły planu, które mają zastosowanie w przypadku danych urządzeń.

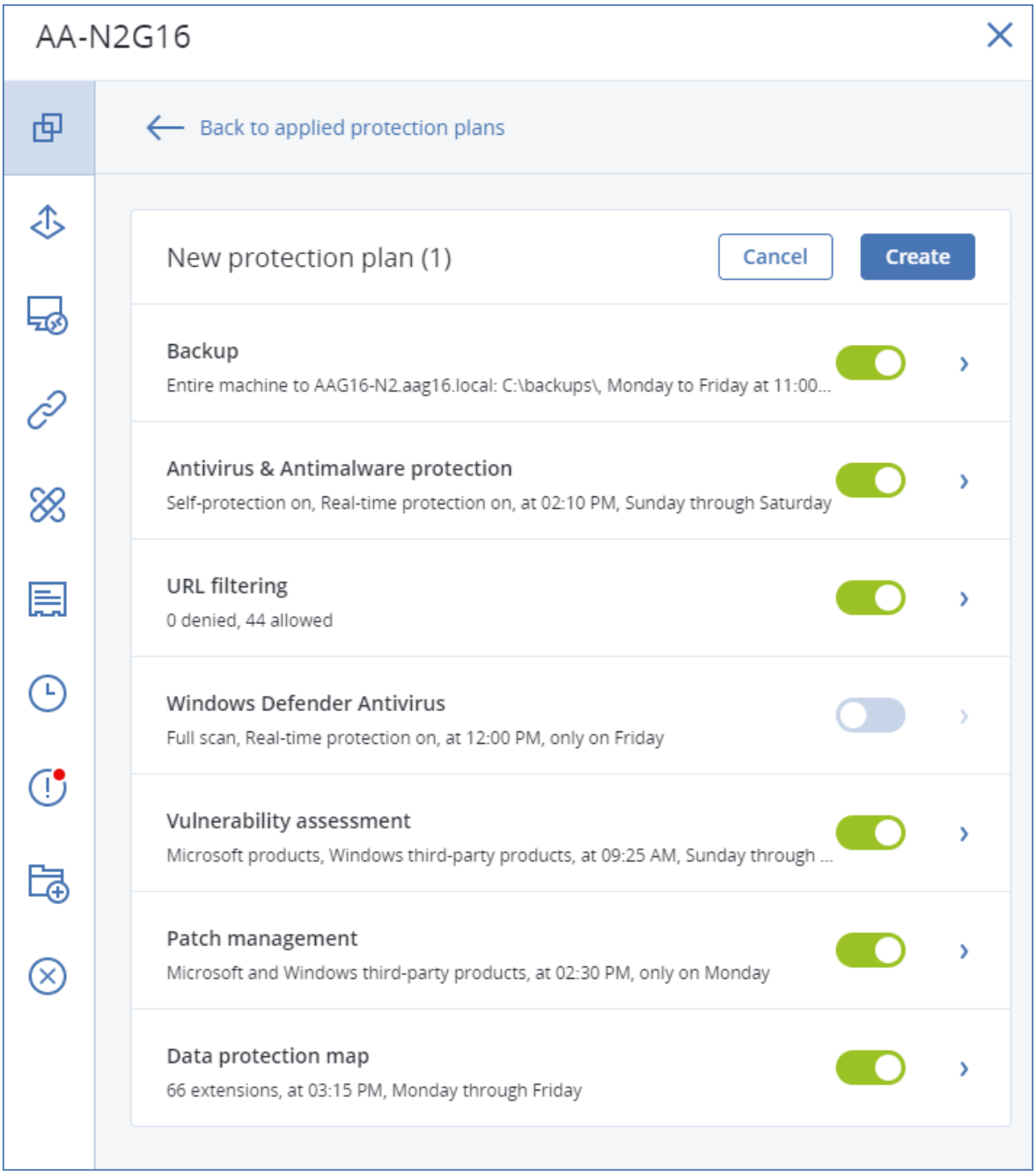
Plan ochrony można utworzyć na dwa sposoby:

- W sekcji **Urządzenia** — wybrać urządzenia, które mają być chronione, a następnie utworzyć dla nich plan.
- W sekcji **Plany** — utworzyć plan, a następnie wybrać komputery, do których ma on zostać zastosowany.

Przyjrzyjmy się bliżej pierwszemu sposobowi.

Aby utworzyć pierwszy plan ochrony

1. W konsoli internetowej Cyber Protect przejdź do sekcji **Urządzenia** > **Wszystkie urządzenia**.
2. Wybierz komputery, które chcesz chronić.
3. Kliknij **Chroń**, a następnie kliknij **Utwórz plan**. Pojawi się plan ochrony z domyślnymi ustawieniami.



4. [Opcjonalnie] Aby zmienić nazwę planu ochrony, kliknij widoczną obok niej ikonę ołówka.
5. [Opcjonalnie] Aby włączyć lub wyłączyć moduł planu ochrony, kliknij przełącznik widoczny obok nazwy modułu.
6. [Opcjonalnie] Aby skonfigurować parametry modułu, kliknij odpowiednią sekcję planu ochrony.
7. Gdy skończysz, kliknij **Utwórz**.

Moduły Kopia zapasowa, Ochrona przed wirusami i złośliwym oprogramowaniem, Ocena luk w zabezpieczeniach, Zarządzanie poprawkami i Mapa ochrony danych można uruchamiać na żądanie, klikając **Uruchom teraz**.

Usuwanie konfliktów między planami

Plan ochrony może mieć jeden z następujących statusów:

- **Aktywne** — plan przypisany do urządzeń i stosowany do nich.
- **Nieaktywne** — plan przypisany do urządzeń, ale wyłączony i niestosowany.

Stosowanie kilku planów do jednego urządzenia

Istnieje możliwość zastosowania kilku planów ochrony do jednego urządzenia. W wyniku tego powstanie kombinacja różnych planów ochrony przypisanych do jednego urządzenia. Można na przykład zastosować jeden plan, który ma włączony tylko moduł Ochrona przed wirusami i złośliwym oprogramowaniem, oraz drugi plan, który ma włączony tylko moduł Kopia zapasowa. Plany ochrony można łączyć tylko wtedy, gdy ich moduły się nie pokrywają. Jeśli te same moduły są włączone w więcej niż jednym planie ochrony, należy rozwiązać konflikty między nimi.

Usuwanie konfliktów między planami

Plan powoduje konflikty z już stosowanymi planami

Jeśli utworzysz nowy plan na potrzeby urządzeń z już stosowanymi planami, które są w konflikcie z nowym planem, możesz usunąć ten konflikt na jeden z następujących sposobów:

- Utwórz nowy plan, zastosuj go i wyłącz wszystkie stosowane plany, które powodują konflikt.
- Utwórz nowy plan i go wyłącz.

Jeśli wyedytujesz nowy plan na potrzeby urządzeń z już stosowanymi planami, które są w konflikcie z wprowadzonymi zmianami, możesz usunąć ten konflikt na jeden z następujących sposobów:

- Zapisz zmiany w planie i wyłącz wszystkie stosowane już plany, które powodują konflikt.
- Zapisz zmiany w planie i go wyłącz.

Plan urządzenia powoduje konflikt z planem grupy

Jeśli urządzenie należy do grupy urządzeń z przypisanym planem grupy i spróbujesz przypisać do tego urządzenia nowy plan, system wyświetli monit o rozwiązanie konfliktu przez wykonanie jednej z następujących czynności:

- Usunięcie urządzenia z grupy i zastosowanie do niego nowego planu.
- Zastosowanie nowego planu do całej grupy lub wyedytowanie bieżącego planu grupy.

Problem z licencją

Limit przypisany do urządzenia musi być dopasowany do planu ochrony, który ma zostać wykonany, zaktualizowany lub zastosowany. Aby rozwiązać problem z licencją, wykonaj jedną z następujących

czynności:

- Wyłącz moduły nieobsługiwane w ramach przypisanego limitu i dalej korzystaj z planu ochrony.
- Ręcznie zmień przypisany limit: przejdź do sekcji **Urządzenia** > **<Konkretne_urządzenie>** > **Szczegóły** > **Limit usług**. Następnie odwołaj bieżący limit i przypisz nowy.

Operacje dotyczące planów ochrony

Informacje na temat tworzenia planu ochrony można znaleźć w sekcji „Tworzenie planu ochrony".

Dostępne działania dotyczące planu ochrony

W odniesieniu do planu ochrony można wykonywać następujące działania:

- Zmienianie nazwy planu
- Włączanie i wyłączanie modułów oraz edytowanie ich ustawień
- Włączanie i wyłączanie planu

  Wyłączony plan nie zostanie wykonany na urządzeniu, do którego został zastosowany.

  Ta czynność jest wygodna dla administratorów, którzy zamierzają później chronić to samo urządzenie za pomocą tego samego planu. Ponieważ plan nie zostaje odwołany z urządzenia, w celu przywrócenia ochrony administrator musi tylko ponownie włączyć plan.
- Stosowanie planu do urządzeń lub grupy urządzeń
- Odwoływanie planu z urządzenia

  Odwołany plan nie będzie już stosowany do danego urządzenia.

  Ta czynność jest wygodna dla administratorów, którzy nie zamierzają już nigdy chronić tego samego urządzenia za pomocą tego samego planu. Aby przywrócić ochronę przy użyciu odwołanego planu, administrator musi znać jego nazwę, wybrać go z listy dostępnych planów, a następnie ponownie zastosować do żądanego urządzenia.
- Importowanie i eksportowanie planu

  Uwaga
  Można zaimportować tylko plany ochrony utworzone w programie Acronis Cyber Protect 15. Plany ochrony utworzone w starszych wersjach są niekompatybilne z programem Acronis Cyber Protect 15.

- Usuwanie planu

Aby zastosować już istniejący plan ochrony

1. Wybierz komputery, które chcesz chronić.
2. Kliknij **Chroń**. Jeśli do wybranych komputerów jest już stosowany plan ochrony, kliknij **Dodaj plan**.
3. W oprogramowaniu zostaną wyświetlone utworzone wcześniej plany ochrony.
4. Wybierz ochronę, której potrzebujesz, a następnie kliknij **Zastosuj**.

Aby edytować plan ochrony

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

Aby odwołać plan ochrony na komputerach

1. Wybierz komputery, na których chcesz odwołać plan ochrony.
2. Kliknij **Chroń**.
3. Jeśli do tych komputerów jest stosowanych kilka planów ochrony, wybierz plan, który chcesz odwołać.
4. Kliknij ikonę wielokropka widoczną obok nazwy planu ochrony, a następnie kliknij **Odwołaj**.

Aby usunąć plan ochrony

1. Wybierz dowolny komputer, do którego jest stosowany plan ochrony przeznaczony do usunięcia.
2. Kliknij **Chroń**.
3. Jeśli do tego komputera jest stosowanych kilka planów ochrony, wybierz plan, który chcesz usunąć.
4. Kliknij ikonę wielokropka widoczną obok nazwy planu ochrony, a następnie kliknij **Usuń**.
   W wyniku tego plan ochrony zostanie odwołany na wszystkich komputerach i całkowicie usunięty z interfejsu internetowego.

Kopia zapasowa

Plan ochrony z włączonym modułem Kopia zapasowa to zestaw reguł określających sposób ochrony konkretnych danych na konkretnym komputerze.

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

Uwaga
Jeśli w przypadku wdrożeń lokalnych na serwerze zarządzania są dostępne tylko licencje wersji Standard, nie można zastosować planu ochrony do więcej niż jednego komputera fizycznego. Każdy komputer fizyczny musi mieć własny plan ochrony.

Aby utworzyć pierwszy plan ochrony z włączonym modułem Kopia zapasowa

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

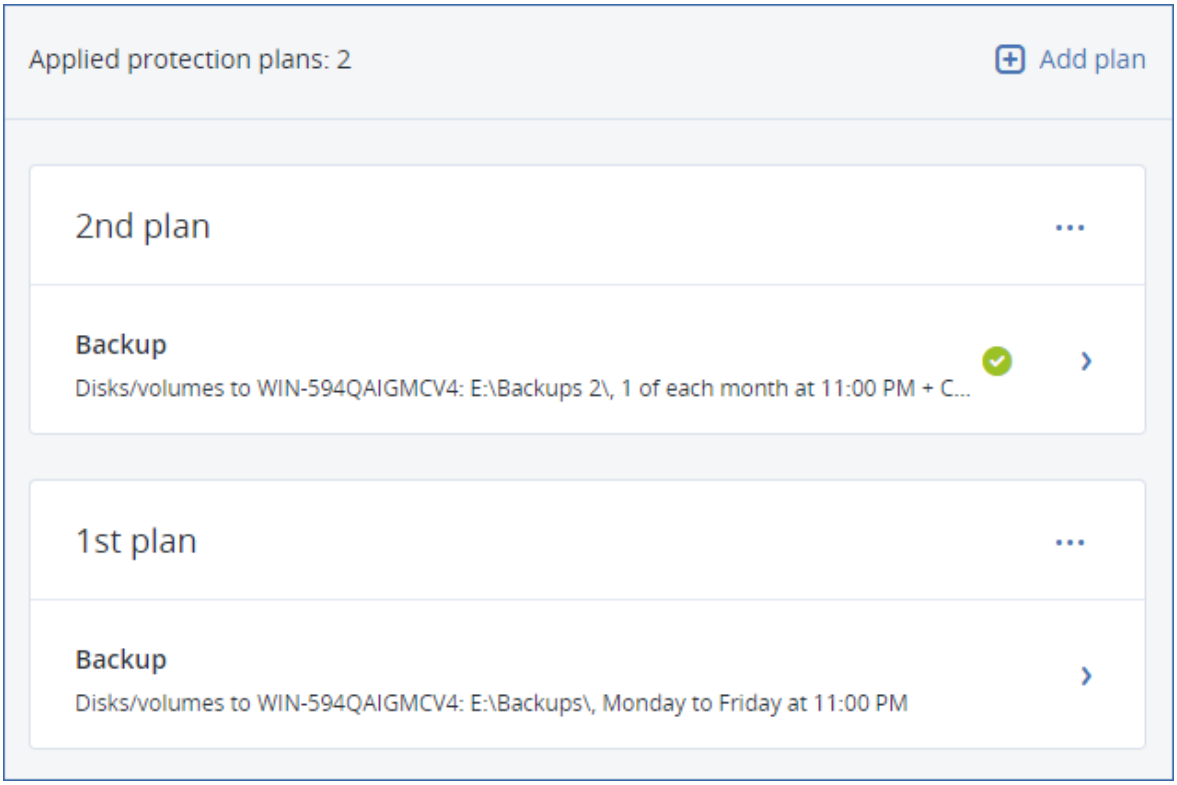
   W oprogramowaniu są wyświetlane plany ochrony stosowane do danego komputera. Jeśli do komputera nie przypisano jeszcze żadnych planów, pojawi się domyślny plan ochrony, który można zastosować. W razie potrzeby można dostosować ustawienia i zastosować ten plan lub

utworzyć nowy.

3. Aby utworzyć nowy plan, kliknij **Utwórz plan**. Włącz moduł **Kopia zapasowa** i rozwiń sekcję ustawień.
4. [Opcjonalnie] Aby zmienić nazwę planu ochrony, kliknij nazwę domyślną.
5. [Opcjonalnie] Aby zmodyfikować parametry modułu Kopia zapasowa, kliknij odpowiednią sekcję na panelu planu ochrony.
6. [Optional] Aby zmodyfikować opcje tworzenia kopii zapasowych, kliknij **Zmień** obok pozycji **Opcje tworzenia kopii zapasowych**.
7. Kliknij **Utwórz**.

Aby zastosować już istniejący plan ochrony

1. Wybierz komputery, których kopie zapasowe chcesz utworzyć.
2. Kliknij **Chroń**. Jeśli do wybranych komputerów jest już stosowany wspólny plan ochrony, kliknij **Dodaj plan**.
   W oprogramowaniu zostaną wyświetlone utworzone wcześniej plany ochrony.



3. Wybierz plan ochrony, który chcesz zastosować.
4. Kliknij **Zastosuj**.

Moduł Kopia zapasowa — ściągawka

Ważne
Niektóre funkcje opisane w tej sekcji są dostępne tylko w przypadku wdrożeń lokalnych.

W poniższej tabeli zestawiono dostępne parametry modułu Kopia zapasowa. Dzięki temu przygotujesz optymalny plan ochrony.

OBIEKTY DO UWZGLĘDNIENIA W KOPII ZAPASOWEJ	ELEMENTY DO UWZGLĘDNIENIA W KOPII ZAPASOWEJ Metody wyboru	MIEJSCE DOCELOWE KOPII ZAPASOWEJ	HARMONOGRAM Schematy tworzenia kopii zapasowych	OKRES PRZECHOWYWANIA

			(nie dotyczy chmury)	
Dyski/woluminy (komputery fizyczne)	Wybór bezpośredni Reguły zasad Filtry plików	Chmura Folder lokalny Folder sieciowy Serwer SFTP* NFS* Secure Zone* Lokalizacja zarządzana* Urządzenie taśmowe*	Zawsze przyrostowa (jednoplikowa)* Zawsze pełne Tygodniowe pełne, dzienne przyrostowe Miesięczne pełne, tygodniowe różnicowe, dzienne przyrostowe (GFS) Niestandardowe (P-D-P)	Według wieku kopii zapasowych (jedna reguła na zestaw kopii zapasowych) Według liczby kopii zapasowych Według łącznego rozmiaru kopii zapasowych Zachowaj w nieskończoność
Dyski/woluminy (maszyny wirtualne)	Reguły zasad Filtry plików	Chmura Folder lokalny Folder sieciowy Serwer SFTP* NFS* Lokalizacja zarządzana* Urządzenie taśmowe*		
Pliki (tylko komputery fizyczne)	Wybór bezpośredni Reguły zasad Filtry plików	Chmura Folder lokalny Folder sieciowy Serwer SFTP* NFS* Secure	Zawsze pełne Tygodniowe pełne, dzienne przyrostowe Miesięczne pełne, tygodniowe różnicowe, dzienne przyrostowe (GFS)	

		Zone* Lokalizacja zarządzana* Urządzenie taśmowe	Zawsze przyrostowa (jednoplikowa)* Niestandardowe (P-D-P)	
Konfiguracja ESXi	Wybór bezpośredni	Folder lokalny Folder sieciowy Serwer SFTP NFS*		
Stan systemu (tylko we wdrożeniach chmurowych)	Wybór bezpośredni	Chmura Folder lokalny Folder sieciowy	Zawsze pełne Tygodniowe pełne, dzienne przyrostowe Niestandardowe (P-P)	
Bazy danych SQL	Wybór bezpośredni	Chmura Folder lokalny Folder sieciowy Lokalizacja zarządzana* Urządzenie taśmowe		
Bazy danych programu Exchange	Wybór bezpośredni			
Skrzynki pocztowe programu Exchange	Wybór bezpośredni	Chmura Folder lokalny Folder sieciowy Lokalizacja zarządzana*	Zawsze przyrostowa (jednoplikowa)	
Skrzynki pocztowe Microsoft 365	Wybór bezpośredni			Według wieku kopii zapasowych (jedna reguła na zestaw kopii zapasowych) Według liczby kopii

				zapasowych Zachowaj w nieskończoność

* Patrz ograniczenia poniżej.

Ograniczenia

Serwer SFTP i urządzenie taśmowe

- Te lokalizacje nie mogą być miejscem docelowym kopii zapasowych komputerów z systemem macOS.
- Te lokalizacje nie mogą być miejscem docelowym kopii zapasowych uwzględniających aplikację.
- Schemat tworzenia kopii zapasowych **Zawsze przyrostowa (jednoplikowa)** jest niedostępny podczas tworzenia kopii zapasowej w tych lokalizacjach.
- Reguła przechowywania **Według łącznego rozmiaru kopii zapasowych** jest niedostępna dla tych lokalizacji.

NFS

- W systemie Windows tworzenie kopii zapasowych w udziałach NFS jest niedostępne.
- Schemat tworzenia kopii zapasowych **Zawsze przyrostowa (jednoplikowa)** plików (komputerów fizycznych) jest niedostępny w przypadku tworzenia kopii zapasowych w udziałach NFS.

Secure Zone

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

Lokalizacja zarządzana

- Zarządzana lokalizacja z włączoną deduplikacją lub szyfrowaniem nie może zostać wybrana jako miejsce docelowe:
  - Jeśli schemat tworzenia kopii zapasowych jest ustawiony jako **Zawsze przyrostowa (jednoplikowa)**
  - Jeśli format kopii zapasowej jest ustawiony jako **Wersja 12**
  - W przypadku kopii zapasowych na poziomie dysku tworzonych w odniesieniu do komputerów z systemem macOS
  - W przypadku kopii zapasowych skrzynek pocztowych programu Exchange i skrzynek pocztowych Microsoft 365.
- Reguła przechowywania **Według łącznego rozmiaru kopii zapasowych** jest niedostępna dla zarządzanych lokalizacji z włączoną deduplikacją.

Zawsze przyrostowa (jednoplikowa)

- Schemat tworzenia kopii zapasowych **Zawsze przyrostowa (jednoplikowa)** jest niedostępny podczas tworzenia kopii zapasowej na serwerze SFTP lub urządzeniu taśmowym.
- Schemat tworzenia kopii zapasowych **Zawsze przyrostowa (jednoplikowa)** plików (komputerów fizycznych) jest dostępny tylko wtedy, gdy główną lokalizacją kopii zapasowych jest magazyn Acronis Cloud.

Według łącznego rozmiaru kopii zapasowych

- Reguła przechowywania **Według łącznego rozmiaru kopii zapasowych** jest niedostępna:
  - Jeśli schemat tworzenia kopii zapasowych jest ustawiony jako **Zawsze przyrostowa (jednoplikowa)**
  - W przypadku tworzenia kopii zapasowej na serwerze SFTP, urządzeniu taśmowym lub zarządzanej lokalizacji z włączoną deduplikacją.

Wybieranie danych do uwzględnienia w kopii zapasowej

Wybieranie całego komputera

W kopii zapasowej całego komputera są uwzględniane wszystkie jego dyski niewymienne.

Aby skonfigurować taką kopię zapasową, w polu **Elementy uwzględniane w kopii zapasowej** wybierz **Cały komputer**.

Ważne
Dyski zewnętrzne, takie jak dyski flash USB lub dyski twarde USB, nie są uwzględniane w kopii zapasowej tworzonej przy użyciu opcji **Cały komputer**. Aby utworzyć kopię zapasową tych dysków, skonfiguruj kopię zapasową przy użyciu opcji **Dyski/woluminy**. Więcej informacji o tworzeniu kopii zapasowej dysków można znaleźć w sekcji "Wybieranie dysków/woluminów" (s. 220).

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 niewymienne.

Uwaga
Folder główny OneDrive jest domyślnie wykluczany z operacji tworzenia kopii zapasowych. W przypadku wybrania określonych plików i folderów OneDrive będą one uwzględniane w kopii zapasowej. Pliki, które nie są dostępne na urządzeniu, będą miały nieprawidłową zawartość w archiwum.

Dyski/woluminy można wybierać na dwa sposoby: bezpośrednio na każdym komputerze lub przy użyciu reguł zasad. Ustawiając filtry plików, można wykluczyć pliki z kopii zapasowej dysku.

Wybór bezpośredni

Wybór bezpośredni jest dostępny tylko w przypadku komputerów fizycznych. Aby umożliwić bezpośrednie wybieranie dysków i woluminów na maszynie wirtualnej, trzeba w jej systemie operacyjnym gościa zainstalować agenta ochrony.

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 ochrony 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 ochrony. 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 dotyczące systemów Windows, Linux i macOS

- `[Wszystkie woluminy]` powoduje wybranie wszystkich woluminów na komputerach z systemem Windows i wszystkich zamontowanych woluminów na komputerach z systemem Linux lub macOS.

Reguły dotyczące systemu Windows

- Litera dysku (na przykład **C:**) powoduje wybranie woluminu z określoną literą dysku.
- `[Woluminy stałe (komputery fizyczne)]` 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.
- `[STARTOWY + SYSTEMOWY]` powoduje wybranie woluminu systemowego i startowych. Ta kombinacja to minimalny zestaw danych, który umożliwia odzyskanie systemu operacyjnego z kopii zapasowej.

- `[DYSK STARTOWY+SYSTEMOWY (komputery fizyczne)]` powoduje wybranie wszystkich woluminów dysku, na których znajdują się wolumin systemowy i woluminy startowe. Jeśli wolumin systemowy i woluminy startowe nie znajdują się na tym samym dysku, nie zostanie wybrana żadna opcja. Ta reguła ma zastosowanie wyłącznie w przypadku komputerów fizycznych.
- `[Dysk 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, podaj jego ścieżkę, która pojawi się po uruchomieniu polecenia `ls /dev/mapper` na koncie użytkownika root. Na przykład:

```
[root@localhost ~]# ls /dev/mapper/
control vg_1-lv1 vg_1-lv2
```

Zostaną wyświetlone dwa woluminy logiczne — **lv1** i **lv2** — należące do grupy woluminów **vg_1**. Aby utworzyć kopię zapasową tych woluminów, wprowadź:

```
/dev/mapper/vg_1-lv1
/dev/mapper/vg-l-lv2
```

Reguły dotyczące systemu macOS

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

Co zawiera kopia zapasowa dysku lub woluminu?

Utworzenie kopii zapasowej dysku lub woluminu polega na zapisaniu całego **systemu plików** dysku lub woluminu wraz z wszystkimi informacjami potrzebnymi do uruchomienia systemu operacyjnego. Z takich kopii zapasowych można odzyskać całe dyski lub woluminy, jak również poszczególne pliki lub foldery.

Jeśli jest włączona opcja **sektor po sektorze" (tryb „surowych" danych)** kopii zapasowej, w kopii zapasowej dysku są zapisywane wszystkie jego sektory. Operacja kopiowania „sektor po sektorze" pozwala tworzyć kopie zapasowe dysków zawierających nierozpoznane lub nieobsługiwane systemy plików oraz dane w innych zastrzeżonych formatach.

Windows

Kopia zapasowa woluminu zawiera wszystkie pliki i foldery wybranego woluminu niezależnie od ich atrybutów (w tym pliki ukryte i systemowe), rekord startowy, tablicę FAT (o ile istnieje), katalog główny i zerową ścieżkę dysku twardego z głównym rekordem startowym (MBR).

Kopia zapasowa dysku zawiera wszystkie woluminy wybranego dysku (w tym woluminy ukryte, takie jak partycje konserwacyjne producenta) oraz ścieżkę zerową głównego rekordu rozruchowego.

Kopia zapasowa dysku ani woluminu (ani kopia na poziomie plików) *nie* zawiera następujących elementów:

- Plik wymiany (pagefile.sys) i plik z zawartością pamięci RAM komputera przechodzącego w stan hibernacji (hiberfil.sys). Po odzyskaniu danych pliki te zostaną ponownie utworzone w odpowiednim miejscu z zerowym rozmiarem.
- Jeśli kopia zapasowa jest tworzona w systemie operacyjnym (inaczej niż w przypadku tworzenia kopii zapasowej na nośnik startowy lub tworzenia kopii zapasowej maszyn wirtualnych z poziomu hiperwizora):
  - Magazyn kopii w tle systemu Windows. Ścieżkę do tego magazynu określa wartość rejestru **VSS Default Provider**, która znajduje się w kluczu rejestru **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\BackupRestore\FilesNotToBackup**. Oznacza to, że od wersji Windows 7 w systemach operacyjnych Windows nie są tworzone kopie zapasowe punktów przywracania systemu Windows.
  - Jeśli jest włączona opcja tworzenia kopii zapasowych **Usługa kopiowania woluminów w tle (VSS)**, obejmuje to pliki i foldery określone w kluczu rejestru **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\BackupRestore\FilesNotToSnapshot**.

Linux

Kopia zapasowa woluminu zawiera wszystkie pliki i katalogi wybranego woluminu niezależnie od ich atrybutów, rekord startowy oraz superblok systemu plików.

Kopia zapasowa dysku zawiera wszystkie woluminy dysku oraz ścieżkę zerową z głównym rekordem rozruchowym.

Mac

Kopia zapasowa dysku lub woluminu przechowuje wszystkie pliki i katalogi wybranego dysku lub woluminu, a także opis układu woluminu.

Wykluczone są następujące elementy:

- Metadane systemu, takie jak dziennik systemu plików indeks funkcji Spotlight
- Kosz
- Kopie zapasowe programu Time Machine

Kopie zapasowe dysków i woluminów komputera Mac są tworzone fizycznie na poziomie pliku. Można odzyskać kopię zapasową dysku lub woluminu bez systemu operacyjnego, ale nie jest dostępny tryb kopii zapasowej sektor po sektorze.

Wybieranie plików/folderów

W przypadku tworzenia kopii zapasowej komputerów fizycznych i maszyn wirtualnych przez agenta zainstalowanego w systemie-gościu jest dostępna kopia zapasowa na poziomie plików.

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.

Uwaga
Folder główny OneDrive jest domyślnie wykluczany z operacji tworzenia kopii zapasowych. W przypadku wybrania określonych plików i folderów OneDrive będą one uwzględniane w kopii zapasowej. Pliki, które nie są dostępne na urządzeniu, będą miały nieprawidłową zawartość w archiwum.

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.

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 ochrony:
   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.
      Tworzenie kopii zapasowych w folderze z anonimowym dostępem nie jest obsługiwane.
   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 ochrony. 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:
  - `[Wszystkie pliki]` powoduje wybranie wszystkich plików we wszystkich woluminach komputera.
  - `[Folder wszystkich profili]` 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**.
  - `/home` powoduje wybranie katalogu głównego zwykłych użytkowników.
  - `/root` powoduje wybranie katalogu głównego użytkownika root.
  - `/usr` powoduje wybranie katalogu wszystkich programów związanych z użytkownikami.
  - `/etc` powoduje wybranie katalogu plików konfiguracyjnych systemu.
- Szablony:

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

Reguły wyboru dotyczące systemu macOS

- Pełna ścieżka pliku lub katalogu.
- Szablony:
  - `[Folder wszystkich profili]` 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**.

Wybieranie stanu systemu

Kopia zapasowa stanu systemu jest dostępna tylko w przypadku komputerów z systemem Windows 7 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

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
- 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.
- Aby utworzyć kopię zapasową konfiguracji środowiska ESXi, agent dla VMware używa połączenia SSH z hostem ESXi przez port TCP 22. Upewnij się, że zapora nie blokuje tego połączenia.
- Trzeba znać hasło do konta „root" na hoście ESXi.

Ograniczenia

- Kopie zapasowe konfiguracji ESXi nie są obsługiwane w przypadku systemu VMware vSphere 7.0.
- Konfiguracji ESXi nie można uwzględnić w kopii zapasowej w chmurze.

Aby wybrać konfigurację ESXi

1. Kliknij **Urządzenia** > **Wszystkie urządzenia**, a następnie wybierz hosty ESXi, które chcesz uwzględnić w kopii zapasowej.
2. Kliknij **Kopia zapasowa**.
3. W obszarze **Elementy uwzględniane w kopii zapasowej** zaznacz **Konfiguracja ESXi**.
4. W polu **Hasło do konta „root" ESXi** określ hasło do konta „root" na każdym z wybranych hostów lub zastosuj jedno hasło do wszystkich hostów.

Ciągła ochrona danych

Ze względu na wydajność kopie zapasowe są zwykle wykonywane w regularnych, ale dość długich odstępach. Jeśli system ulegnie nagłej awarii, zmiany danych wprowadzone między utworzeniem ostatniej kopii zapasowej a wystąpieniem awarii systemu zostaną utracone.

Funkcja **Ciągła ochrona danych** umożliwia nieprzerwane tworzenie kopii zapasowych zmian wybranych danych między zaplanowanymi operacjami tworzenia kopii zapasowych:

- Przez śledzenie zmian w określonych plikach/folderach
- Przez śledzenie zmian w plikach modyfikowanych przez określone aplikacje

Spośród danych wybranych do uwzględniania w kopiach zapasowych można wybrać konkretne pliki, które mają zostać objęte ciągłą ochroną danych. System będzie uwzględniać w kopii zapasowej każdą zmianę wprowadzoną w tych plikach. Pliki te będzie można odzyskać w stanie z czasu ostatniej zmiany.

Obecnie funkcja **Ciągła ochrona danych** jest obsługiwana w przypadku następujących systemów operacyjnych:

- Windows 7 lub nowszy
- Windows Server 2008 R2 lub nowszy

Obsługiwany system plików: tylko NTFS, tylko foldery lokalne (foldery udostępnione nie są obsługiwane).

Opcja **Ciągła ochrona danych** nie współdziała z opcją **Kopia zapasowa aplikacji**.

Uwaga
Funkcje różnią się w zależności od wersji. Niektóre funkcje opisane w tej dokumentacji mogą być niedostępne w ramach używanej licencji. Szczegółowe informacje na temat funkcji zawartych w poszczególnych wersjach można znaleźć w artykule Porównanie wersji programu Acronis Cyber Protect 15, w tym wdrożenia chmurowego.

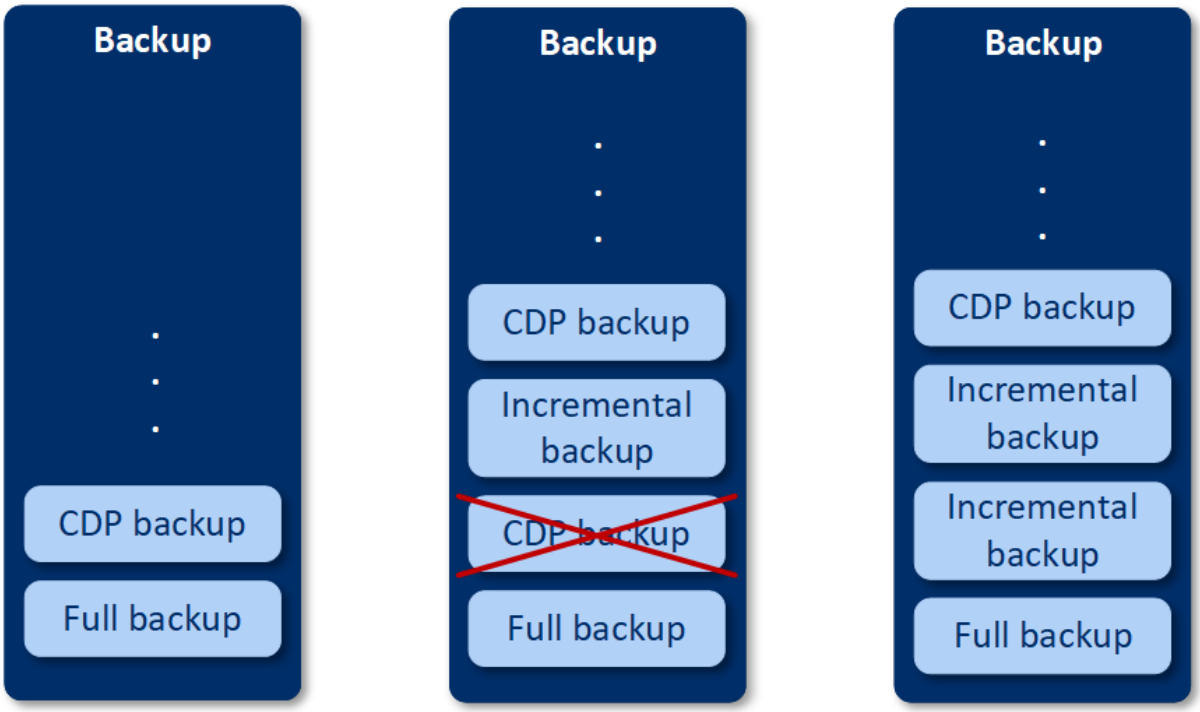
Sposób działania

Kopię zapasową tworzoną w sposób ciągły będziemy nazywać „kopią zapasową CDP". Aby została utworzona kopia zapasowa CDP, najpierw musi zostać utworzona pełna lub przyrostowa kopia zapasowa.

Po pierwszym uruchomieniu planu ochrony z włączonym modułem Kopia zapasowa i funkcją **Ciągła ochrona danych** jest tworzona pełna kopia zapasowa. Zaraz potem zostanie utworzona kopia zapasowa CDP wybranych lub zmienionych plików/folderów. Kopia zapasowa CDP zawsze zawiera najnowszą wersję wybranych danych. Jeśli wprowadzisz zmiany w wybranych plikach/folderach, nie zostanie utworzona nowa kopia zapasowa CDP — wszystkie zmiany są rejestrowane w tej samej kopii zapasowej CDP.

Gdy przyjdzie czas na utworzenie zaplanowanej przyrostowej kopii zapasowej, dotychczasowa kopia zapasowa CDP zostanie usunięta, a po utworzeniu przyrostowej kopii zapasowej zostanie utworzona nowa kopia zapasowa CDP.

Dzięki temu kopia zapasowa CDP zawsze jest ostatnia w ciągu kopii zapasowych i zawiera najnowszy, faktyczny stan chronionych plików/folderów.



Jeśli już masz plan ochrony z włączonym modułem Kopia zapasowa i zdecydujesz się włączyć funkcję **Ciągła ochrona danych**, to zaraz po włączeniu tej opcji zostanie utworzona kopia zapasowa CDP, ponieważ ciąg kopii zapasowych już zawiera pełne kopie zapasowe.

Obsługiwane źródła danych i lokalizacje docelowe w ramach ciągłej ochrony danych

Aby ciągła ochrona danych działała jak należy, trzeba wskazać odpowiednie elementy w ramach źródeł danych:

Elementy uwzględniane w kopii zapasowej	Elementy uwzględniane w kopii zapasowej
Cały komputer	Pliki/foldery lub aplikacje
Dyski/woluminy	Dyski/woluminy oraz pliki/foldery lub aplikacji
Pliki/foldery	Pliki/foldery Aplikacje (ale nie obowiązkowo)

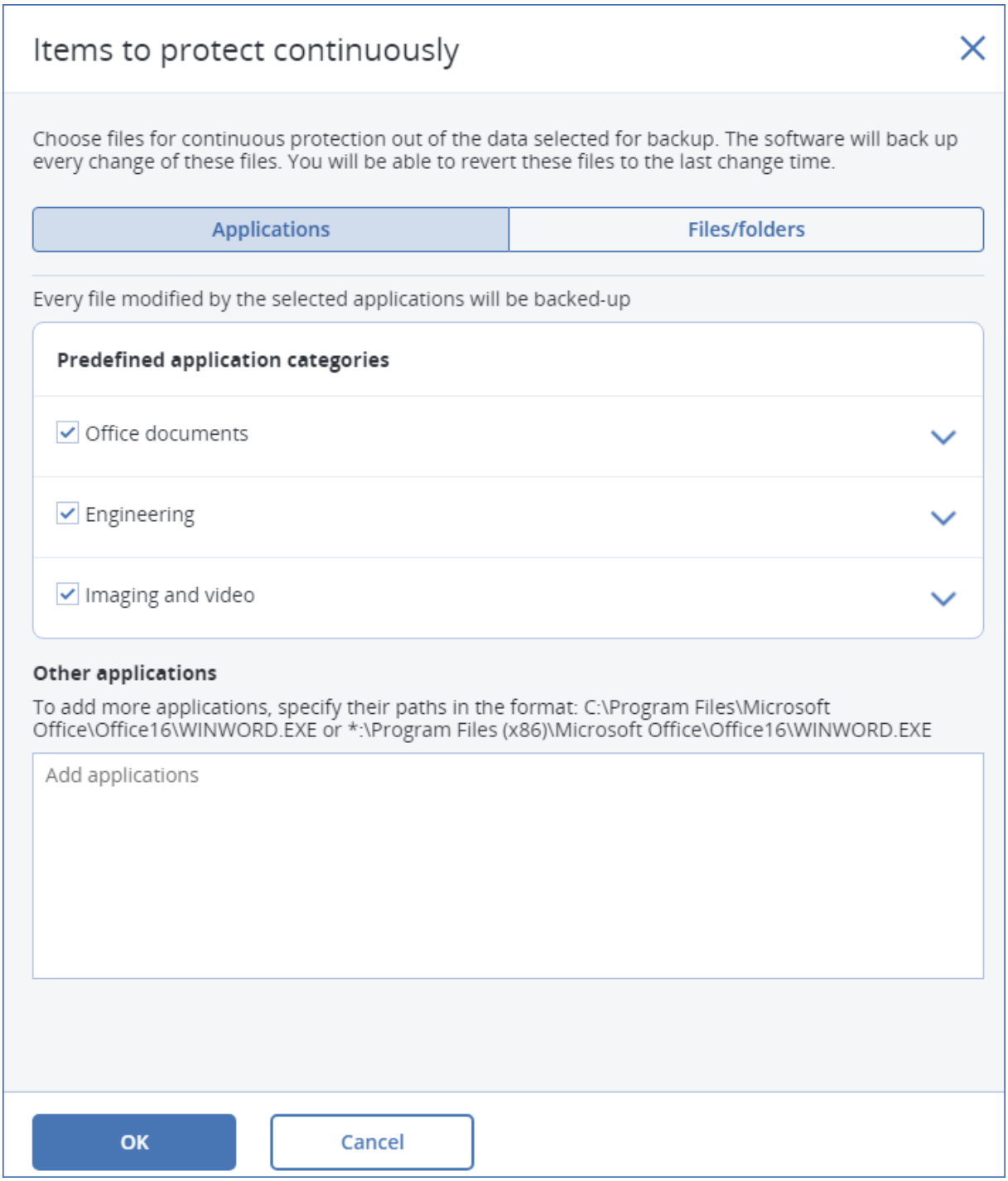
W ramach ciągłej ochrony danych obsługiwane są następujące docelowe lokalizacje kopii zapasowych:

- Folder lokalny
- Folder sieciowy
- Lokalizacja zdefiniowana za pomocą skryptu

- Chmura
- Acronis Cyber Infrastructure

Aby objąć urządzenie ciągłą ochroną danych

1. W konsoli internetowej Cyber Protect utwórz plan ochrony z włączonym modułem **Kopia zapasowa**.
2. Włącz opcję **Ciągła ochrona danych (CDP)**.
3. Określ **Elementy do objęcia ciągłą ochroną**:
   - **Aplikacje** (w kopii zapasowej zostanie uwzględniony każdy plik zmieniony przez wybrane aplikacje). Warto użyć tej opcji, aby tworzyć kopie zapasowe CDP dokumentów pakietu Office.



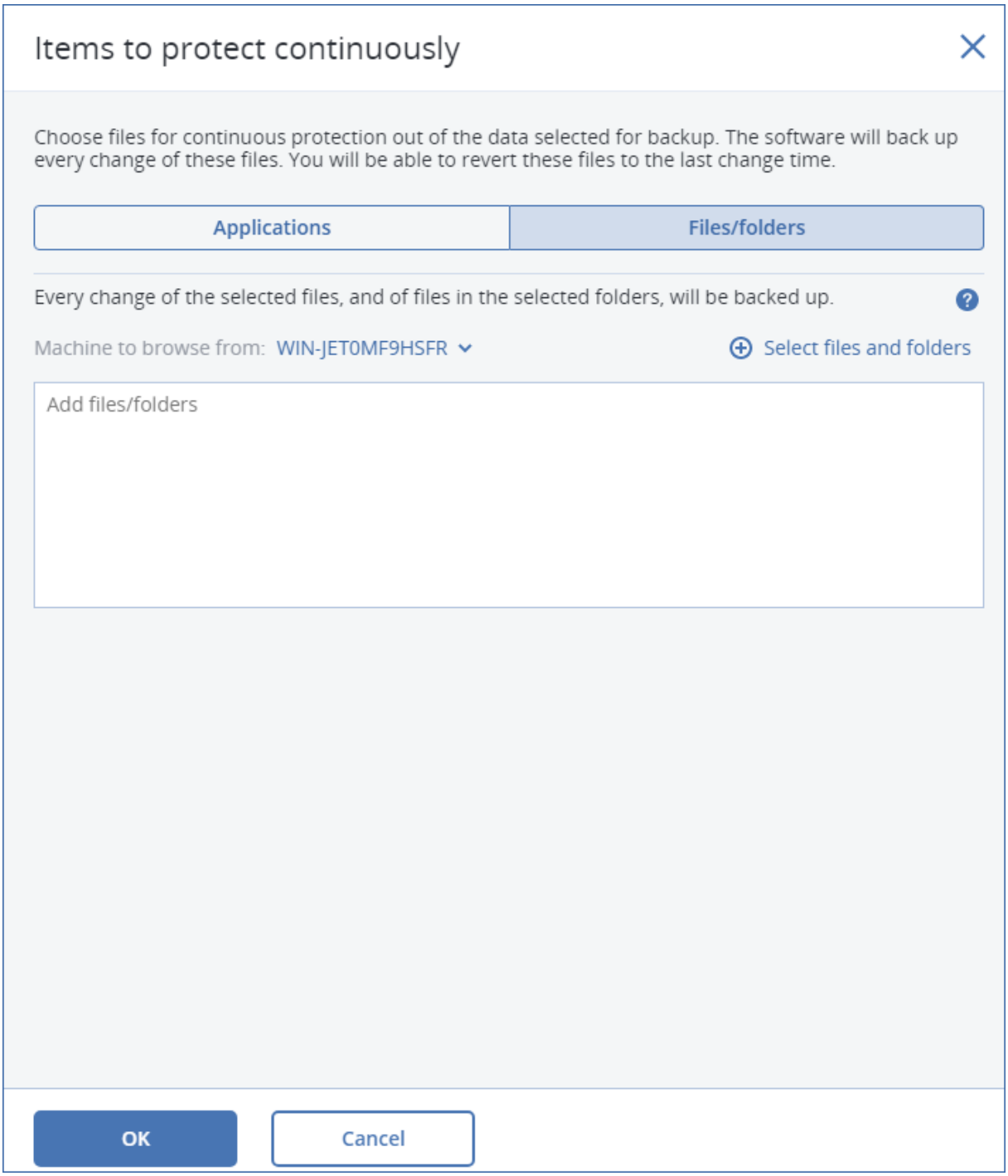
- Możesz wybrać aplikacje z gotowych kategorii lub wskazać inne aplikacje, definiując ścieżki do ich plików wykonywalnych. Użyj jednego z następujących formatów:

  `C:\Program Files\Microsoft Office\Office16\WINWORD.EXE`

  LUB

  `*:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE`

  - **Pliki/foldery** (w kopii zapasowej zostanie uwzględniony każdy zmieniony plik ze wskazanych lokalizacji). Warto użyć tej opcji, aby objąć ochroną stale zmieniane pliki i foldery.



1. **Komputer używany do przeglądania** — wskaż komputer, którego pliki/foldery chcesz objąć ciągłą ochroną danych.
   Kliknij **Wybierz pliki i foldery** aby wybrać pliki/foldery na wskazanym komputerze.

   Ważne
   jeśli ręcznie podajesz cały folder, którego pliki będą stale uwzględniane w kopii zapasowej, użyj tzw. maski (symbolu wieloznacznego), na przykład:
   Poprawna ścieżka: D:\Data*
   Niepoprawna ścieżka: D:\Data\

W polu tekstowym można też określić reguły wybierania plików/folderów do uwzględniania w kopiach zapasowych. Więcej informacji na temat definiowania reguł można znaleźć w sekcji „Wybieranie plików/folderów”. Gdy skończysz, kliknij **Gotowe**.

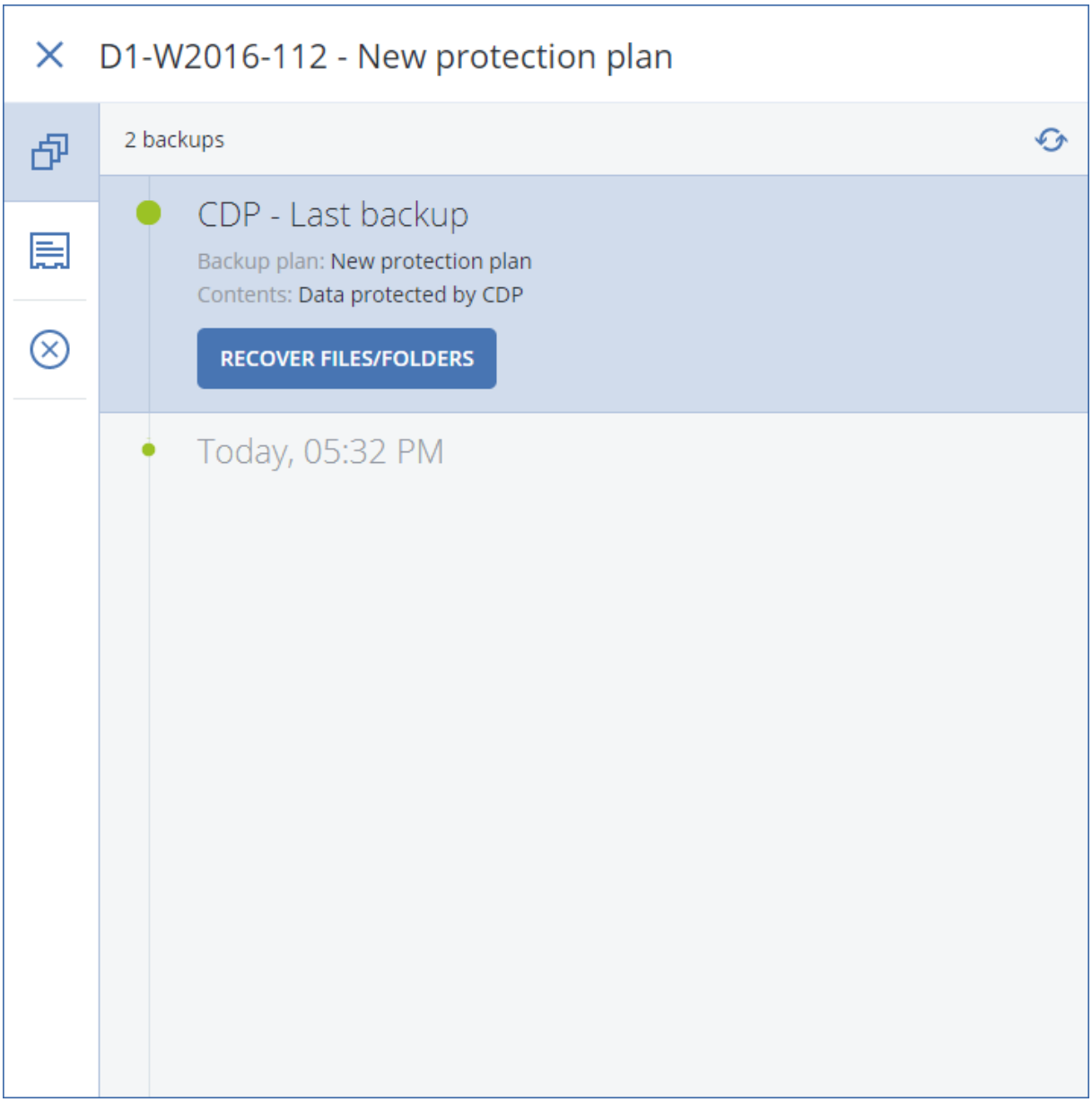
2. Kliknij **Utwórz**.

W wyniku tego do wybranego komputera zostanie przypisany plan ochrony z włączoną ciągłą ochroną danych. Po pierwszej zwykłej kopii zapasowej będą w sposób ciągły tworzone kopie zapasowe zawierające najnowsze wersje danych objętych ciągłą ochroną. W kopii zapasowej będą uwzględniane dane wskazane zarówno za pomocą opcji Aplikacje, jak i za pomocą opcji Pliki/foldery.

Dane ciągle uwzględniane w kopii zapasowej są przechowywane zgodnie z zasadami przechowywania określonymi na potrzeby modułu Kopia zapasowa.

Jak rozróżnić kopie zapasowe tworzone w sposób ciągły

Kopie zapasowe tworzone w sposób ciągły mają prefiks „CDP”.



Jak odzyskać cały komputer do ostatniego stanu

Aby móc odzyskać cały komputer do ostatniego stanu, możesz skorzystać z opcji **Ciągła ochrona danych (CDP)** dostępnej w module Kopia zapasowa planu ochrony.

Z kopii zapasowej CDP można odzyskać cały komputer albo pliki/foldery. W pierwszym przypadku wynikiem operacji będzie cały komputer w najnowszym stanie, w drugim — pliki/foldery w najnowszym stanie.

Wybieranie miejsca docelowego

Ważne
Niektóre funkcje opisane w tej sekcji są dostępne tylko w przypadku wdrożeń lokalnych.

Aby wybrać lokalizację kopii zapasowej

1. Kliknij **Miejsce docelowe kopii zapasowej**.
2. Wykonaj jedną z następujących czynności:
   - Wybierz wcześniej używaną lub wstępnie zdefiniowaną lokalizację kopii zapasowej.
   - Kliknij **Dodaj lokalizację**, a następnie określ nową lokalizację kopii zapasowej:

Obsługiwane lokalizacje

- **Chmura**

  Kopie zapasowe będą przechowywane w chmurowym centrum danych.
- **Folder lokalny**

  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. Poświadczenia te można w każdej chwili zmienić, klikając ikonę klucza obok nazwy folderu.

  Tworzenie kopii zapasowych w folderze z anonimowym dostępem nie jest obsługiwane.
- **Acronis Cyber Infrastructure**

  Acronis Cyber Infrastructure może służyć jako wysoce niezawodny, zdefiniowany programowo magazyn z funkcją nadmiarowości danych i automatycznego naprawiania się. Magazyn ten można skonfigurować jako bramę na potrzeby zapisywania kopii zapasowych w chmurze Microsoft Azure lub w jednym z szerokiej gamy rozwiązań magazynowych zgodnych z chmurą S3 lub Swift. Magazyn też może korzystać z rozwiązań zaplecza NFS. Więcej informacji można znaleźć w sekcji „Informacje o programie Acronis Cyber Infrastructure”.

  Ważne

  Tworzenie kopii zapasowych w rozwiązaniu Acronis Cyber Infrastructure jest niedostępne w przypadku komputerów z systemem macOS.

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

  Sprawdź, czy na komputerze z systemem Linux, na którym jest zainstalowany agent dla systemu Linux, jest też zainstalowany pakiet nfs-utils.

  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)

  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 partycji Secure Zone”.
- **SFTP**

  Wpisz nazwę lub adres serwera SFTP. Obsługiwane są następujące notacje:

  `sftp://<serwer>`

  `sftp://<serwer>/<folder>`

  Po wprowadzeniu nazwy użytkownika i hasła można przeglądać foldery na serwerze.

  W przypadku obu notacji można również określić port, nazwę użytkownika oraz hasło:

  `sftp://<serwer>:<port>/<folder>`

  `sftp://<nazwa użytkownika>@<serwer>:<port>/<folder>`

  `sftp://<nazwa użytkownika>:<haslo>@<serwer>:<port>/<folder>`

  W przypadku nieokreślenia numeru portu zostanie użyty port 22.

  Użytkownicy, dla których skonfigurowano dostęp SFTP bez podania hasła, nie mogą tworzyć kopii zapasowych na serwerze SFTP.

  Tworzenie kopii zapasowych na serwerach FTP jest nieobsługiwane.

Zaawansowane opcje magazynu

- **Zdefiniowana za pomocą skryptu** (dostępne w przypadku komputerów z systemem Windows)

  Kopie zapasowej poszczególnych komputerów można przechowywać w folderze zdefiniowanym za pomocą skryptu. Oprogramowanie obsługuje skrypty napisane w języku JScript, VBScript lub Python 3.5. Wdrażając plan ochrony, oprogramowanie uruchamia skrypt na każdym komputerze. Wynikiem działania skryptu w przypadku każdego komputera powinna być ścieżka folderu lokalnego lub sieciowego. Jeśli folder nie istnieje, zostanie utworzony (ograniczenie: skrypty napisane w języku Python nie mogą tworzyć folderów w udziałach sieciowych). Na karcie **Magazyn kopii zapasowych** każdy folder jest pokazywany jako osobna lokalizacja kopii zapasowych.

  W obszarze **Typ skryptu** wybierz typ skryptu (**JScript**, **VBScript** lub **Python**), a następnie zaimportuj lub skopiuj i wklej skrypt. W przypadku folderów sieciowych podaj poświadczenia dostępu z uprawnieniami do odczytu/zapisu.

  Przykłady:

- Wynikiem działania poniższego skryptu **JScript** jest lokalizacja kopii zapasowych dla komputera w formacie `\\bkpsrv\<nazwa komputera>`:

  ```
  WScript.Echo("\\\\bkpsrv\\" + WScript.CreateObject
  ("WScript.Network").ComputerName);
  ```

- Wynikiem działania poniższego skryptu **JScript** jest lokalizacja kopii zapasowych w folderze na komputerze, na którym uruchomiono skrypt:

  ```
  WScript.Echo("C:\\Backup");
  ```

  Uwaga
  Wielkość liter w ścieżce lokalizacji w tych skryptach ma znaczenie. Dlatego `C:\Backup` i `C:\backup` są widoczne w konsoli internetowej Cyber Protect jako różne lokalizacje. Ponadto jako litery dysku należy użyć wielkiej litery.

- Wynikiem działania poniższego skryptu **VBScript** jest lokalizacja kopii zapasowych dla komputera w formacie `\\bkpsrv\<nazwa komputera>`:

  ```
  WScript.Echo("\\bkpsrv\" + WScript.CreateObject("WScript.Network").ComputerName)
  ```

W rezultacie kopie zapasowe poszczególnych komputerów będą zapisywane w folderze o tej samej nazwie na serwerze **bkpsrv**.

- **Węzeł magazynowania**

  Węzeł magazynowania to serwer przeznaczony do optymalizacji użycia różnych zasobów (takich jak pojemność magazynu firmowego, przepustowości sieci i obciążenia procesorów serwerów produkcyjnych) wymaganych do ochrony danych przedsiębiorstwa. Cel ten jest osiągany dzięki organizowaniu lokalizacji służących jako dedykowane magazyny kopii zapasowych przedsiębiorstwa (lokalizacje zarządzane) i zarządzaniu nimi.

  Program umożliwia wybór wcześniej utworzonej lokalizacji lub utworzenie nowej lokalizacji przez kliknięcie **Dodaj lokalizację** > **Węzeł magazynowania**. Aby uzyskać informacje na temat tych ustawień, zobacz „Dodawanie lokalizacji zarządzanej”.

  Może zostać wyświetlony monit o określenie nazwy użytkownika i hasła w celu uzyskania dostępu do węzła magazynowania. Na komputerze, na którym jest zainstalowany węzeł magazynowania, członkowie następujących grup systemu Windows mają dostęp do wszystkich zarządzanych lokalizacji w węźle magazynowania:

  - **Administratorzy**
  - **Acronis ASN Remote Users**

    Grupa ta jest tworzona automatycznie podczas instalacji węzła magazynowania. Domyślnie ta grupa jest pusta. Można ręcznie dodać do niej użytkowników.

- **Taśma**

  Jeśli urządzenie taśmowe jest podłączone do komputera uwzględnionego w kopii zapasowej lub do węzła magazynowania, na liście lokalizacji zostanie pokazana domyślna pula taśm. Ta pula jest tworzona automatycznie.

Program umożliwia wybór puli domyślnej lub utworzenie nowej puli przez kliknięcie **Dodaj lokalizację** > **Taśma**. Aby uzyskać informacje na temat ustawień puli, zobacz „Tworzenie puli”.

Secure Zone — informacje

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 normalna lokalizacja jest tymczasowo niedostępna albo podłączona poprzez 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

- strefy Secure Zone nie można utworzyć na komputerze Mac.
- 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).
- 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.

Jak utworzenie strefy Secure Zone wpływa na dysk

- Strefa Secure Zone jest zawsze 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.

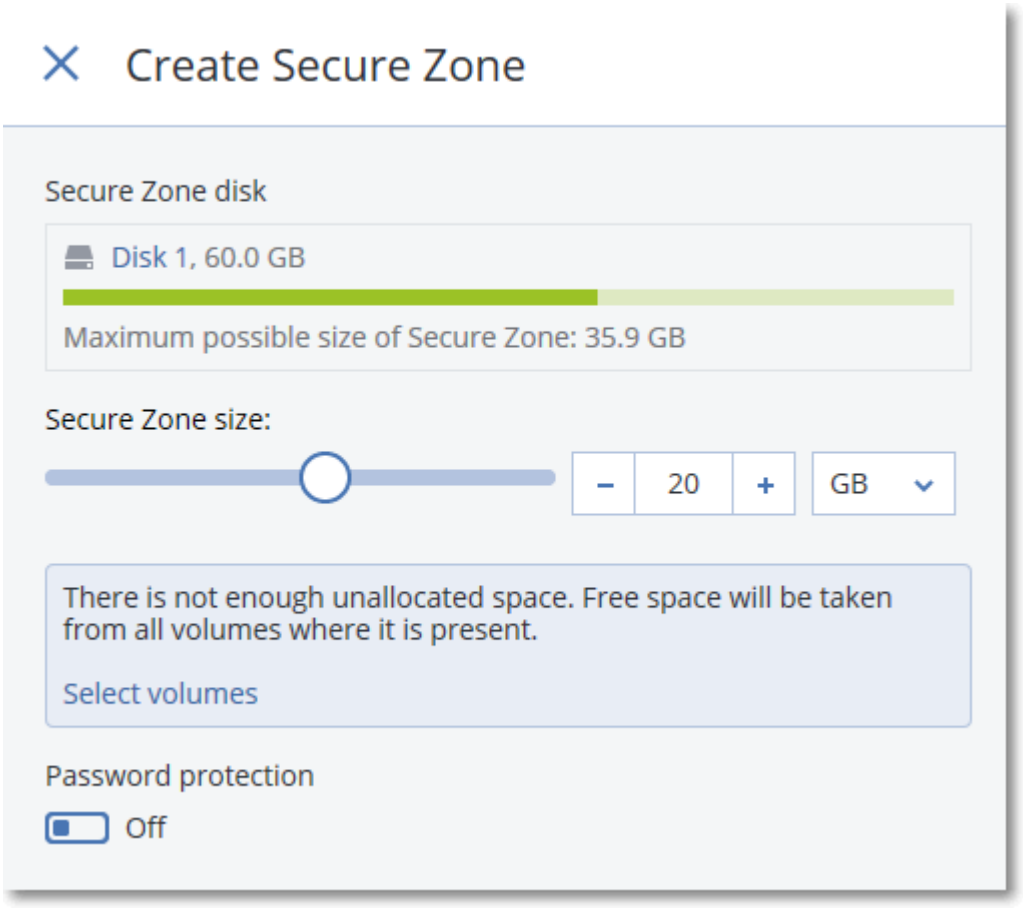
- Na woluminie powinno jednak pozostać wolne miejsce, wymagane do prawidłowego działania systemu operacyjnego i aplikacji (na przykład do tworzenia plików tymczasowych). Oprogramowanie nie zmniejszy rozmiaru woluminu, na którym ilość wolnego miejsca jest lub stałaby się mniejsza niż 25 procent rozmiaru 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 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 jest uruchamiany system, wymaga ponownego uruchomienia komputera.

Jak utworzyć strefę Secure Zone

1. Wybierz komputer, na którym chcesz utworzyć strefę Secure Zone.
2. Kliknij **Szczegóły** > **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.



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 ochrony 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 opcję **Szczegóły**.
3. Kliknij ikonę koła zębatego widoczną obok partycji **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.

Informacje o platformie Acronis Cyber Infrastructure

Program Acronis Cyber Protect 15 obsługuje integrację z rozwiązaniem Acronis Cyber Infrastructure 3.5 Update 5 lub nowszym.

Tworzenie kopii zapasowych w rozwiązaniu Acronis Cyber Infrastructure jest niedostępne w przypadku komputerów z systemem macOS.

Wdrażanie

Aby korzystać z rozwiązania Acronis Cyber Infrastructure, należy je wdrożyć lokalnie na serwerze fizycznym. Aby w pełni korzystać z możliwości tego rozwiązania, warto zastosować co najmniej pięć serwerów fizycznych. Jeśli potrzebujesz tylko funkcji bramy, możesz użyć jednego serwera fizycznego lub wirtualnego albo skonfigurować klaster bramy z dowolną liczbą serwerów.

Dopilnuj, aby ustawienia czasu serwera zarządzania i rozwiązania Acronis Cyber Infrastructure były zsynchronizowane. Ustawienia czasu rozwiązania Acronis Cyber Infrastructure można skonfigurować podczas wdrożenia. Domyślnie jest włączona synchronizacja czasu przy użyciu protokołu NTP (Network Time Protocol).

Istnieje możliwość wdrożenia kilku instancji rozwiązania Acronis Cyber Infrastructure i zarejestrowania ich na serwerze zarządzania.

Rejestracja

Rejestracja jest przeprowadzana w interfejsie internetowym rozwiązania Acronis Cyber Infrastructure. Rejestracji rozwiązania Acronis Cyber Infrastructure mogą dokonywać tylko administratorzy organizacji i tylko w ramach organizacji. Po zarejestrowaniu magazyn ten będzie dostępny dla wszystkich jednostek organizacyjnych. Można go dodać jako lokalizację kopii zapasowych do dowolnej jednostki lub do organizacji.

Operacja odwrotna (wyrejestrowanie) jest przeprowadzana w interfejsie rozwiązania Acronis Cyber Protect. Kliknij **Ustawienia** > **Węzły magazynowania**, kliknij wymaganą instancję rozwiązania Acronis Cyber Infrastructure, a następnie kliknij **Usuń**.

Dodawanie lokalizacji kopii zapasowych

Do jednostki lub organizacji można dodać tylko jedną lokalizację kopii zapasowych na instancję rozwiązania Acronis Cyber Infrastructure. Lokalizacja dodana na poziomie jednostki jest dostępna dla tej jednostki i administratorów organizacji. Lokalizacja dodana na poziomie organizacji jest dostępna tylko dla administratorów organizacji.

Podczas dodawania lokalizacji należy utworzyć i wprowadzić jej nazwę. Jeśli zechcesz dodać istniejącą już lokalizację do nowego lub innego serwera zarządzania, zaznacz pole wyboru **Użyj istniejącej już lokalizacji**, kliknij **Przeglądaj** i wybierz lokalizację z listy.

Jeśli na serwerze zarządzania zarejestrowano kilka instancji rozwiązania Acronis Cyber Infrastructure, podczas dodawania lokalizacji można wybrać jedną z tych instancji.

Schematy tworzenia kopii zapasowych, operacje oraz ograniczenia

Bezpośredni dostęp do rozwiązania Acronis Cyber Infrastructure z nośnika startowego nie jest obsługiwany. Aby korzystać z rozwiązania Acronis Cyber Infrastructure, zarejestruj nośnik na serwerze zarządzania i zarządzaj nim za pomocą konsoli internetowej Cyber Protect.

Dostęp do rozwiązania Acronis Cyber Infrastructure przy użyciu interfejsu wiersza polecenia nie jest obsługiwany.

Jeśli chodzi o dostępne schematy tworzenia kopii zapasowych i operacje na kopiach zapasowych, rozwiązanie Acronis Cyber Infrastructure przypomina chmurę. Jedyna różnica polega na tym, że kopie zapasowe można replikować *z* rozwiązania Acronis Cyber Infrastructure podczas wykonywania planu ochrony.

Dokumentacja

Pełna dokumentacja rozwiązania Acronis Cyber Infrastructure jest dostępna w witrynie internetowej firmy Acronis.

Harmonogram

Ważne
Niektóre funkcje opisane w tej sekcji są dostępne tylko w przypadku wdrożeń lokalnych.

W harmonogramie używane są ustawienia czasu (w tym strefy czasowej) systemu operacyjnego, w którym jest zainstalowany agent. Strefę czasową agenta dla VMware (urządzenie wirtualne) można skonfigurować w interfejsie agenta.

Jeśli na przykład plan ochrony ma zostać uruchomiony o godzinie 21:00 i zastosowany do kilku komputerów znajdujących się w różnych strefach czasowych, to operacja tworzenia kopii zapasowej na każdym komputerze rozpocznie się o godzinie 21:00 czasu lokalnego.

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.

Możesz zaplanować rozpoczęcie tworzenia kopii zapasowej w zależności od zdarzenia zamiast od czasu. W tym celu zaznacz typ zdarzenia w selektorze harmonogramu. Aby uzyskać więcej informacji, zobacz „Planowanie według zdarzeń”.

Ważne
Pierwsza tworzona kopia zapasowa będzie pełna, a więc i jej utworzenie potrwa najdłużej. 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 ochrony, który obejmuje harmonogram oraz metody tworzenia kopii zapasowych.

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

- **Zawsze przyrostowa (jednoplikowa)**
  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.
  W przypadku tych kopii zapasowych będzie stosowany nowy format jednoplikowych kopii zapasowych[1].
  Ten schemat jest niedostępny podczas tworzenia kopii zapasowej na urządzeniu taśmowym lub serwerze SFTP.
- **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

[1]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. Ten format jednoplikowej kopii zapasowej nie jest dostępny w przypadku wykonywania kopii zapasowej do lokalizacji nieobsługujących odczytu i zapisu z dostępem losowym, takich jak serwery SFTP.

ikonę koła zębatego, a następnie **Opcje tworzenia kopii zapasowych** > **Tygodniowa kopia zapasowa**).

- **Miesięczne pełne, tygodniowe różnicowe, dzienne przyrostowe (GFS)**

  Domyślnie przyrostowe kopie zapasowe są tworzone codziennie od poniedziałku do piątku. Różnicowe kopie zapasowe są tworzone co sobotę. Pełne kopie zapasowe są tworzone pierwszego dnia każdego miesiąca. Możesz zmodyfikować te harmonogramy i godzinę rozpoczęcia tworzenia kopii zapasowej.

  Ten schemat tworzenia kopii zapasowych jest wyświetlany w panelu planu ochrony jako schemat **Niestandardowe**.
- **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.

Za pomocą dowolnego schematu tworzenia kopii zapasowych możesz zaplanować rozpoczęcie tworzenia kopii zapasowej w zależności od zdarzenia zamiast od czasu. W tym celu zaznacz typ zdarzenia w selektorze harmonogramu. Aby uzyskać więcej informacji, zobacz „Planowanie według zdarzeń”.

Dodatkowe opcje planowania

W przypadku każdego miejsca docelowego można wykonać następujące czynności:

- Określić warunki rozpoczęcia tworzenia kopii zapasowej tak, aby zaplanowana kopia zapasowa została utworzona tylko, jeśli są spełnione warunki. Aby uzyskać więcej informacji, zobacz „Warunki rozpoczęcia”.
- 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 ochrony na tych komputerach. Pozostaje ona niezmienna do chwili ewentualnej edycji planu ochrony 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.

- Kliknij **Pokaż więcej**, aby uzyskać dostęp do następujących opcji:
  - **Jeżeli komputer jest wyłączony, uruchom pominięte zadania przy uruchamianiu** (opcja domyślnie wyłączona)
  - **Zapobiegaj włączaniu trybu uśpienia lub hibernacji podczas tworzenia kopii zapasowych** (opcja domyślnie włączona)
    Ta opcja działa tylko na komputerach z systemem Windows.
  - **Wznów pracę z trybu uśpienia lub hibernacji, aby rozpocząć planowaną operację tworzenia kopii zapasowej** (opcja domyślnie wyłączona)
    Ta opcja działa tylko na komputerach z systemem Windows. Ta opcja nie działa, gdy komputer jest wyłączony, tj. nie powoduje ona użycia funkcji Wake-on-LAN.

Harmonogram jest oparty na zdarzeniach.

Konfigurując harmonogram planu ochrony, możesz wybrać typ zdarzenia w selektorze harmonogramu. Tworzenie kopii zapasowej zostanie uruchomione zaraz po wystąpieniu zdarzenia.

Możesz wybrać jedno z poniższych zdarzeń:

- **Po upływie określonego czasu od utworzenia ostatniej kopii zapasowej**
  Jest to czas od ostatniego pomyślnego zakończenia operacji tworzenia kopii zapasowej w ramach tego samego planu ochrony. Program umożliwia określenie czasu.

  Uwaga
  Ponieważ harmonogram jest oparty na pomyślnym utworzeniu kopii zapasowej, to w przypadku niepowodzenia operacji tworzenia kopii zapasowej nie uruchomi on zadania ponownie, dopóki operator nie uruchomi planu ręcznie i plan ten nie zakończy się pomyślnie.

- **Gdy użytkownik zaloguje się w systemie**
  Domyślnie zalogowanie się dowolnego użytkownika spowoduje zainicjowanie tworzenia kopii zapasowej. Dowolnego użytkownika można zmienić na określone konto użytkownika.
- **Gdy użytkownik wyloguje się z systemu**
  Domyślnie wylogowanie się dowolnego użytkownika spowoduje zainicjowanie tworzenia kopii zapasowej. Dowolnego użytkownika można zmienić na określone konto użytkownika.

  Uwaga
  Tworzenie kopii zapasowej nie zostanie uruchomione podczas zamknięcia systemu, ponieważ zamknięcie systemu nie jest tożsame z wylogowaniem użytkownika.

- **Podczas uruchamiania systemu**

- **Podczas zamknięcia systemu**
- **Po zdarzeniu zarejestrowanym w dzienniku zdarzeń systemu Windows**
  Należy określić właściwości tego zdarzenia.

W poniższej tabeli wymieniono zdarzenia dostępne w przypadku różnych danych w systemach Windows, Linux i macOS.

OBIEKTY DO UWZGLĘDNIENIA W KOPII ZAPASOWEJ	Po upływie określonego czasu od utworzenia ostatniej kopii zapasowej	Gdy użytkownik zaloguje się w systemie	Gdy użytkownik wyloguje się z systemu	Podczas uruchamiania systemu	Podczas wyłączania systemu	Po zdarzeniu zarejestrowanym w dzienniku zdarzeń systemu Windows
Dyski/woluminy lub pliki (na komputerach fizycznych)	Windows, Linux, macOS	Windows	Windows	Windows, Linux, macOS	Windows	Windows
Dyski/woluminy (maszyny wirtualne)	Windows, Linux	–	–	–	–	–
Konfiguracja ESXi	Windows, Linux	–	–	–	–	–
Skrzynki pocztowe Microsoft 365	Windows	–	–	–	–	Windows
Bazy danych i skrzynki pocztowe programu Exchange	Windows	–	–	–	–	Windows
Bazy danych SQL	Windows	–	–	–	–	Windows

Po zdarzeniu zarejestrowanym w dzienniku zdarzeń systemu Windows

Zadanie tworzenia kopii zapasowej można zaplanować tak, aby było uruchamiane po zarejestrowaniu określonego zdarzenia systemu Windows w jednym z dzienników zdarzeń, takim jak dziennik **aplikacji**, **zabezpieczeń** lub **systemu**.

Można na przykład skonfigurować plan ochrony, który zapewni automatyczne wykonanie pilnej pełnej kopii zapasowej danych, gdy tylko system Windows wykryje zbliżającą się awarię dysku twardego.

Aby przeglądać zdarzenia i wyświetlać właściwości zdarzeń, użyj przystawki **Podgląd zdarzeń** dostępnej w konsoli **Zarządzanie komputerem**. Aby otworzyć dziennik **zabezpieczeń**, musisz należeć do grupy **administratorów**.

Właściwości zdarzenia

Nazwa dziennika

Określa nazwę dziennika. Wybierz z listy nazwę dziennika standardowego (**Aplikacja**, **Zabezpieczenia** lub **System**) lub wpisz nazwę dziennika, na przykład: **Sesje Microsoft Office**

Źródło zdarzenia

Określa źródło zdarzenia, zwykle wskazując program lub komponent systemu, który spowodował zdarzenie, na przykład: **dysk**.

Źródło zdarzenia, które zawiera określony ciąg znaków, spowoduje uruchomienie zaplanowanej operacji tworzenia kopii zapasowej. W ramach tej opcji nie jest uwzględniana wielkość znaków. Dzięki temu w przypadku podania ciągu **usług** operację tworzenia kopii zapasowej wywoła zarówno źródło zdarzeń **Menedżer kontroli usługi**, jak i **Usługa czasu**.

Typ zdarzenia

Określa typ zdarzenia: **Błąd**, **Ostrzeżenie**, **Informacja**, **Powodzenie inspekcji** lub **Niepowodzenie inspekcji**.

Identyfikator zdarzenia

Określa numer zdarzenia, który zwykle umożliwia identyfikację konkretnego rodzaju zdarzeń wśród zdarzeń o takim samym źródle.

Na przykład zdarzenie **Błąd** o źródle **dysk** i identyfikatorze **7** występuje, gdy system Windows wykryje na dysku nieprawidłowy blok, natomiast zdarzenie **Błąd** o źródle **dysk** i identyfikatorze **15** występuje, gdy dysk nie jest jeszcze gotowy do użycia.

Przykład: Awaryjna kopia zapasowa po wykryciu „uszkodzonych sektorów”

Jeżeli na dysku twardym nagle pojawi się jeden lub więcej uszkodzonych sektorów, oznacza to, że wkrótce nastąpi awaria dysku twardego. Załóżmy, że chcesz utworzyć plan ochrony, który spowoduje utworzenie kopii zapasowej danych z dysku twardego, gdy tylko wystąpi taka sytuacja.

Gdy system Windows wykryje na dysku twardym uszkodzony sektor, rejestruje zdarzenie o źródle **disk** i identyfikatorze **7** w dzienniku **System**. Typ tego zdarzenia to **Błąd**.

Tworząc plan, wpisz lub wybierz następujące parametry w sekcji **Harmonogram**:

- **Nazwa dziennika**: **System**
- **Źródło zdarzenia**: **disk**
- **Typ zdarzenia**: **Błąd**
- **Identyfikator zdarzenia**: **7**

Ważne
Aby zapewnić wykonanie tego zadania kopii zapasowej mimo obecności uszkodzonych sektorów, należy określić ignorowanie takich sektorów podczas zadania tworzenia kopii zapasowej. W tym celu w sekcji **Opcje tworzenia kopii zapasowej** przejdź do pozycji **Obsługa błędów**, a następnie zaznacz pole wyboru **Ignoruj sektory uszkodzone**.

Warunki rozpoczęcia

Te ustawienia zwiększają elastyczność harmonogramu, ponieważ dzięki nim kopie zapasowe mogą być wykonywane zgodnie z określonymi warunkami. W przypadku określenia wielu warunków wszystkie muszą zostać spełnione, aby została uruchomiona operacja tworzenia kopii zapasowej. Warunki rozpoczęcia nie są uwzględniane, jeśli operacja tworzenia kopii zapasowej zostanie uruchomiona ręcznie.

Aby uzyskać dostęp do tych ustawień, kliknij **Pokaż więcej** podczas konfigurowania harmonogramu planu ochrony.

Zachowanie harmonogramu w przypadku niespełnienia warunku (lub jednego z wielu warunków) jest zdefiniowane przez opcję tworzenia kopii zapasowych Warunki rozpoczęcia tworzenia kopii zapasowych. Jeśli warunki pozostają niespełnione przez zbyt długi czas i dalsze opóźnianie tworzenia kopii zapasowej staje się ryzykowne, można wyznaczyć czas, po upływie którego kopia zapasowa zostanie wykonana niezależnie od sytuacji.

W poniższej tabeli wymieniono warunki uruchomienia zadania dostępne w przypadku różnych danych w systemach Windows, Linux i macOS.

OBIEKTY DO UWZGLĘDNIENIA W KOPII ZAPASOWEJ	Dyski/woluminy lub pliki (na komputerach fizycznych)	Dyski/woluminy (maszyny wirtualne)	Konfiguracja ESXi	Skrzynki pocztowe Microsoft 365	Bazy danych i skrzynki pocztowe programu Exchange	Bazy danych SQL

Użytkownik jest bezczynny	Windows	–	–	–	–	–
Host lokalizacji kopii zapasowej jest dostępny	Windows, Linux, macOS	Windows, Linux	Windows, Linux	Windows	Windows	Windows
Użytkownicy są wylogowani	Windows	–	–	–	–	–
Mieści się w przedziale czasu	Windows, Linux, macOS	Windows, Linux	–	–	–	–
Oszczędzaj baterię	Windows	–	–	–	–	–
Nie uruchamiaj przy połączeniu taryfowym	Windows	–	–	–	–	–
Nie uruchamiaj przy połączeniu z następującym i sieciami Wi-Fi	Windows	–	–	–	–	–
Sprawdź adres IP urządzenia	Windows	–	–	–	–	–

Użytkownik jest bezczynny

„Użytkownik jest bezczynny” oznacza, że na komputerze jest uruchomiony wygaszacz ekranu lub komputer jest zablokowany.

Przykład

Kopia zapasowa jest tworzona na komputerze codziennie o 21:00, najlepiej wtedy, kiedy użytkownik jest bezczynny. Jeśli użytkownik nadal jest aktywny o 23:00, kopia zapasowa jest tworzona pomimo wszystko.

- Harmonogram: codziennie, uruchamiane codziennie. Uruchom o: **21:00**.
- Warunek: **Użytkownik jest bezczynny**.
- Warunki rozpoczęcia tworzenia kopii zapasowych: **Poczekaj na spełnienie warunków. Rozpocznij tworzenie kopii zapasowej niezależnie od warunków po 2** godz.

Wskutek tego:

(1) Jeśli użytkownik przejdzie w stan bezczynności przed 21:00, tworzenie kopii zapasowej rozpocznie się o 21:00.

(2) Jeśli użytkownik przejdzie w stan bezczynności między 21:00 a 23:00, tworzenie kopii zapasowej rozpocznie się natychmiast po przejściu w stan bezczynności.

(3) Jeśli użytkownik będzie nadal aktywny o 23:00, tworzenie kopii zapasowej rozpocznie się pomimo tego o 23:00.

Host lokalizacji kopii zapasowej jest dostępny

„Host lokalizacji kopii zapasowej jest dostępny" oznacza, że komputer będący hostem lokalizacji docelowej przechowywania kopii zapasowych jest dostępny przez sieć.

Ten warunek jest skuteczny w przypadku folderów sieciowych, magazynu chmurowego i lokalizacji zarządzanych przez węzeł magazynowania.

Ten warunek nie dotyczy dostępności samej lokalizacji, a jedynie hosta. Jeśli na przykład host jest dostępny, ale folder sieciowy na tym hoście nie jest udostępniony lub poświadczenia folderu nie są już ważne, ten warunek nadal jest uznawany za spełniony.

Przykład

W każdym dniu roboczym o 21:00 jest wykonywana kopia zapasowa danych do folderu sieciowego. Jeśli komputer będący hostem folderu nie jest dostępny w danej chwili (na przykład z powodu konserwacji), należy pominąć tworzenie kopii zapasowej i zaczekać na zaplanowane rozpoczęcie następnego dnia roboczego.

- Harmonogram: codziennie, uruchamiane od poniedziałku do piątku. Uruchom o: **21:00**.
- Warunek: **Host lokalizacji kopii zapasowej jest dostępny.**
- Warunki rozpoczęcia tworzenia kopii zapasowych: **Pomiń zaplanowaną operację tworzenia kopii zapasowej.**

Wskutek tego:

(1) Jeśli host będzie dostępny o 21:00, natychmiast rozpocznie się tworzenie kopii zapasowej.

(2) Jeśli o 21:00 host nie będzie dostępny, tworzenie kopii zapasowej rozpocznie się następnego dnia roboczego, jeśli host będzie dostępny.

(3) Jeśli host nigdy nie jest dostępny o 21:00 w dni robocze, nigdy nie rozpocznie się tworzenie kopii zapasowej.

Użytkownicy są wylogowani

Umożliwia wstrzymanie tworzenia kopii zapasowej do momentu wylogowania wszystkich użytkowników z systemu Windows.

Przykład

Tworzenie kopii zapasowej rozpoczyna się o 20:00 w każdy piątek. Preferowana jest sytuacja, w której wszyscy użytkownicy są wylogowani. Jeśli jeden z użytkowników jest nadal zalogowany o 23:00, tworzenie kopii zapasowej rozpoczyna się pomimo tego.

- Harmonogram: co tydzień, w piątki. Uruchom o: **20:00**.
- Warunek: **Użytkownicy są wylogowani**.
- Warunki rozpoczęcia tworzenia kopii zapasowych: **Poczekaj na spełnienie warunków**. **Rozpocznij tworzenie kopii zapasowej niezależnie od warunków po 3** godz.

Wskutek tego:

(1) Jeśli o 20:00 wszyscy użytkownicy będą wylogowani, tworzenie kopii zapasowej rozpocznie się o 20:00.

(2) Jeśli ostatni użytkownik wyloguje się między 20:00 a 23:00, tworzenie kopii zapasowej rozpocznie się natychmiast po jego wylogowaniu.

(3) Jeśli jakikolwiek użytkownik będzie nadal zalogowany o 23:00, tworzenie kopii zapasowej rozpocznie się o 23:00.

Zadanie mieści się w przedziale czasu

Ogranicza godzinę rozpoczęcia tworzenia kopii zapasowej do określonego przedziału czasu.

Przykład

Firma używa różnych lokalizacji w tej samej sieciowej pamięci masowej do tworzenia kopii zapasowych danych użytkowników i serwerów. Dzień roboczy rozpoczyna się o 08:00 i kończy o 17:00. Kopię zapasową danych użytkowników należy tworzyć jak tylko użytkownicy się wylogują, ale nie wcześniej niż o 16:30. Codziennie o 23:00 jest tworzona kopia zapasowa serwerów firmy. W związku z tym tworzenie kopii zapasowej danych użytkowników powinno zostać zakończone przed tą godziną, aby zwolnić przepustowość sieci. Zakłada się, że tworzenie kopii zapasowej danych użytkowników zajmuje co najwyżej godzinę, więc najpóźniejszą godziną rozpoczęcia tworzenia kopii zapasowej jest 22:00. Jeśli użytkownik jest nadal zalogowany w określonym przedziale czasu lub wyloguje się o dowolnej innej godzinie — nie wykonuj kopii zapasowej danych użytkownika, tj. pomiń wykonanie kopii zapasowej.

- Zdarzenie: **Gdy użytkownik wyloguje się z systemu**. Określ konto użytkownika: **Dowolny użytkownik**.
- Warunek: **Mieści się w przedziale czasu** od **16:30** do **22:00**.

- Warunki rozpoczęcia tworzenia kopii zapasowych: **Pomiń zaplanowaną operację tworzenia kopii zapasowej.**

Wskutek tego:

(1) Jeśli użytkownik wyloguje się między 16:30 a 22:00, tworzenie kopii zapasowej rozpocznie się natychmiast po wylogowaniu.

(2) Jeśli użytkownik wyloguje się o dowolnej innej porze, tworzenie kopii zapasowej zostanie pominięte.

Oszczędzaj baterię

Umożliwia zapobieganie tworzeniu kopii zapasowej w sytuacji, gdy urządzenie (laptop lub tablet) nie jest podłączone do źródła zasilania. Wartość opcji tworzenia kopii zapasowej Warunki rozpoczęcia tworzenia kopii zapasowych określa, czy pominięta operacja tworzenia kopii zapasowej ma się rozpocząć po podłączeniu urządzenia do źródła zasilania. Dostępne są następujące opcje:

- **Nie uruchamiaj przy zasilaniu z baterii**
  Tworzenie kopii zapasowej rozpocznie się tylko wtedy, gdy urządzenie jest podłączone do źródła zasilania.
- **Uruchom przy zasilaniu z baterii, jeśli poziom naładowania przekracza**
  Tworzenie kopii zapasowej rozpocznie się, jeśli urządzenie jest podłączone do źródła zasilania lub poziom naładowania baterii przewyższa określoną wartość.

Przykład

W każdym dniu roboczym o 21:00 jest wykonywana kopia zapasowa danych. Jeśli urządzenie nie jest podłączone do źródła zasilania (na przykład wtedy, gdy użytkownik bierze udział w późnym spotkaniu), można pominąć operację tworzenia kopii zapasowej, aby oszczędzać baterię, i poczekać, aż użytkownik podłączy urządzenie do źródła zasilania.

- Harmonogram: codziennie, uruchamiane od poniedziałku do piątku. Uruchom o: 21:00.
- Warunek: **Oszczędzaj baterię**, **Nie uruchamiaj przy zasilaniu z baterii**.
- Warunki rozpoczęcia tworzenia kopii zapasowych: **Poczekaj na spełnienie warunków**.

Wskutek tego:

(1) Gdy nadchodzi godzina 21:00 i urządzenie jest podłączone do źródła zasilania, natychmiast rozpoczyna się tworzenie kopii zapasowej.

(2) Gdy nadchodzi godzina 21:00 i urządzenie działa na baterii, tworzenie kopii zapasowej rozpoczyna się, gdy tylko urządzenie zostanie podłączone do źródła zasilania.

Nie uruchamiaj przy połączeniu taryfowym

Umożliwia zapobieganie utworzeniu kopii zapasowej (w tym kopii zapasowej dysku lokalnego), jeśli urządzenie jest podłączone do Internetu przez połączenie skonfigurowane w systemie Windows jako

taryfowe. Aby uzyskać więcej informacji na temat połączeń taryfowych w systemie Windows, zobacz https://support.microsoft.com/en-us/help/17452/windows-metered-internet-connections-faq.

Dodatkowym rozwiązaniem zapobiegającym tworzeniu kopii zapasowych za pośrednictwem hotspotów telefonii komórkowej jest automatyczne włączanie warunku **Nie uruchamiaj przy połączeniu z następującymi sieciami Wi-Fi** w przypadku włączenia warunku **Nie uruchamiaj przy połączeniu taryfowym**. Domyślnie są określone następujące nazwy sieci: „android„, „telefon", „komórkowa" oraz „modem". Nazwy te można usuwać z listy kliknięciem symbolu X.

Przykład

W każdym dniu roboczym o 21:00 jest wykonywana kopia zapasowa danych. Jeśli urządzenie jest podłączone do Internetu przy użyciu połączenia taryfowego (na przykład wtedy, gdy użytkownik jest w podróży służbowej), można pominąć operację tworzenia kopii zapasowej, aby zredukować ruch w sieci, i poczekać na zaplanowane rozpoczęcie tej operacji w następnym dniu roboczym.

- Harmonogram: codziennie, uruchamiane od poniedziałku do piątku. Uruchom o: 21:00.
- Warunek: **Nie uruchamiaj przy połączeniu taryfowym**
- Warunki rozpoczęcia tworzenia kopii zapasowych: **Pomiń zaplanowaną operację tworzenia kopii zapasowej.**

Wskutek tego:

(1) Gdy nadchodzi godzina 21:00 i urządzenie nie jest podłączone do Internetu przez połączenie taryfowe, natychmiast rozpoczyna się tworzenie kopii zapasowej.

(2) Gdy nadchodzi godzina 21:00 i urządzenie jest podłączone do Internetu przez połączenie taryfowe, tworzenie kopii zapasowej rozpoczyna się w następnym dniu roboczym.

(3) Jeśli urządzenie zawsze jest podłączone do Internetu przez połączenie taryfowe o godzinie 21:00 w dni robocze, tworzenie kopii zapasowej się nie rozpoczyna.

Nie uruchamiaj przy połączeniu z następującymi sieciami Wi-Fi

Umożliwia zapobieganie utworzeniu kopii zapasowej (w tym kopii zapasowej dysku lokalnego), jeśli urządzenie jest podłączone do którejkolwiek z określonych sieci bezprzewodowych. Można określić nazwy sieci Wi-Fi, znane również jako identyfikatory SSID.

Ograniczenie to ma zastosowanie do wszystkich sieci mających w nazwie określony ciąg znaków (wielkość liter jest rozróżniana). Jeśli na przykład określisz nazwę sieci „telefon", tworzenie kopii zapasowej się nie rozpocznie, gdy urządzenie jest podłączone do jednej z następujących sieci: „telefon Joli", „telefon_wifi" lub „wifi_z_TELEFONU".

Ten warunek przydaje się do zapobiegania tworzeniu kopii zapasowych, gdy urządzenie jest podłączone do Internetu przez hotspot telefonii komórkowej.

Dodatkowym rozwiązaniem zapobiegającym tworzeniu kopii zapasowych za pośrednictwem hotspotów telefonii komórkowej jest automatyczne włączanie warunku **Nie uruchamiaj przy połączeniu z następującymi sieciami Wi-Fi** w przypadku włączenia warunku **Nie uruchamiaj**

przy połączeniu taryfowym. Domyślnie są określone następujące nazwy sieci: „android„, „telefon”, „komórkowa” oraz „modem”. Nazwy te można usuwać z listy kliknięciem symbolu X.

Przykład

W każdym dniu roboczym o 21:00 jest wykonywana kopia zapasowa danych. Jeśli urządzenie jest podłączone do Internetu przy użyciu hotspota telefonii komórkowej (na przykład wtedy, gdy laptop działa w trybie tetheringu), można pominąć operację tworzenia kopii zapasowej i poczekać na zaplanowane rozpoczęcie tej operacji w następnym dniu roboczym.

- Harmonogram: codziennie, uruchamiane od poniedziałku do piątku. Uruchom o: 21:00.
- Warunek: **Nie uruchamiaj przy połączeniu z następującymi sieciami**, **Nazwa sieci**: `<SSID sieci hotspota>`.
- Warunki rozpoczęcia tworzenia kopii zapasowych: **Pomiń zaplanowaną operację tworzenia kopii zapasowej.**

Wskutek tego:

(1) Gdy nadchodzi godzina 21:00 i komputer nie jest podłączony do określonej sieci, natychmiast rozpoczyna się tworzenie kopii zapasowej.

(2) Gdy nadchodzi godzina 21:00 i komputer jest podłączony do określonej sieci, tworzenie kopii zapasowej rozpoczyna się w następnym dniu roboczym.

(3) Jeśli komputer zawsze jest podłączony do określonej sieci o godzinie 21:00 w dni robocze, tworzenie kopii zapasowej się nie rozpoczyna.

Sprawdź adres IP urządzenia

Umożliwia zapobieganie utworzeniu kopii zapasowej (w tym kopii zapasowej dysku lokalnego), jeśli którykolwiek z adresów IP urządzenia znajduje się w określonym zakresie adresów IP lub poza nim. Dostępne są następujące opcje:

- **Uruchom, jeśli jest spoza zakresu adresów IP**
- **Uruchom, jeśli jest w zakresie adresów IP**

W przypadku każdej z tych opcji można określić kilka zakresów. Obsługiwane są tylko adresy IPv4.

Ten warunek przydaje się w sytuacji, gdy użytkownik jest za granicą, ponieważ pozwala uniknąć wysokich opłat za transmisję danych. Ponadto ułatwia zapobieganie tworzeniu kopii zapasowych przy użyciu połączenia z wirtualną siecią prywatną (VPN).

Przykład

W każdym dniu roboczym o 21:00 jest wykonywana kopia zapasowa danych. Jeśli urządzenie jest podłączone do sieci firmowej przez tunel VPN (np. wtedy, gdy użytkownik pracuje z domu), można pominąć operację tworzenia kopii zapasowej i poczekać, aż użytkownik przyniesie urządzenie do biura.

- Harmonogram: codziennie, uruchamiane od poniedziałku do piątku. Uruchom o: 21:00.
- Warunek: **Sprawdź adres IP urządzenia**, **Uruchom, jeśli jest spoza zakresu adresów IP**, **Od**: `<początek zakresu adresów IP sieci VPN>`, **Do**: `<konie zakresu adresów IP sieci VPN>`.
- Warunki rozpoczęcia tworzenia kopii zapasowych: **Poczekaj na spełnienie warunków**.

Wskutek tego:

(1) Gdy nadchodzi godzina 21:00 i adres IP komputera nie znajduje się w określonym zakresie, natychmiast rozpoczyna się tworzenie kopii zapasowej.

(2) Gdy nadchodzi godzina 21:00 i adres IP komputera znajduje się w określonym zakresie, tworzenie kopii zapasowej rozpoczyna się, gdy tylko urządzenie uzyska adres IP niebędący adresem sieci VPN.

(3) Jeśli adres IP komputera zawsze znajduje się w określonym zakresie o godzinie 21:00 w dni robocze, tworzenie kopii zapasowej się nie rozpoczyna.

Reguły przechowywania

Ważne
Niektóre funkcje opisane w tej sekcji są dostępne tylko w przypadku wdrożeń lokalnych.

1. Kliknij **Okres przechowywania**.
2. W polu **Czyszczenie** wybierz jedną z następujących opcji:
   - **Według wieku kopii zapasowych** (domyślna)
     Określ czas przechowywania kopii zapasowych utworzonych w ramach planu ochrony. Domyślnie reguły przechowywania określa się dla każdego zestawu kopii zapasowych[1] 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.
   - **Według łącznego rozmiaru kopii zapasowych**
     Określ maksymalny łączny rozmiar przechowywanych kopii zapasowych.

[1]Grupa kopii zapasowych, do których można zastosować odrębną regułę przechowywania. W przypadku niestandardowego schematu tworzenia kopii zapasowych 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. 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 zapasowa. Jeśli tygodniowa kopia zapasowa jest pierwszą kopią zapasową utworzoną po rozpoczęciu miesiąca, jest ona uznawana za miesięczną kopię zapasową. W takiej sytuacji tygodniowa kopia zapasowa zostanie utworzona w wybrany dzień następnego tygodnia. Dzienną kopią zapasową jest pierwsza kopia zapasowa utworzona po rozpoczęciu dnia, chyba że spełnia warunki definicji miesięcznej lub tygodniowej kopii zapasowej. Godzinną kopią zapasową jest pierwsza kopia zapasowa utworzona po rozpoczęciu godziny, chyba że spełnia warunki definicji miesięcznej, tygodniowej lub dziennej kopii zapasowej.

W przypadku korzystania ze schematu tworzenia kopii zapasowych **Zawsze przyrostowa (jednoplikowa)** oraz podczas tworzenia kopii zapasowej na serwerze SFTP lub na urządzeniu taśmowym to ustawienie jest niedostępne.

- **Przechowuj kopie zapasowe bezterminowo**

3. Wybierz czas rozpoczęcia wykonywania czyszczenia:
   - **Po utworzeniu kopii zapasowej** (domyślnie)

     Reguły przechowywania będą stosowane po utworzeniu nowej kopii zapasowej.
   - **Przed utworzeniem kopii zapasowej**

     Reguły przechowywania będą stosowane przed utworzeniem nowej kopii zapasowej.

     To ustawienie jest niedostępne podczas tworzenia kopii zapasowych klastrów programu Microsoft SQL Server lub Microsoft Exchange Server.

Co jeszcze warto wiedzieć

- Ostatnia kopia zapasowa utworzona w ramach planu ochrony jest zachowywana we wszystkich przypadkach, chyba że skonfigurowano regułę przechowywania wymagającą wyczyszczenia kopii zapasowych przed rozpoczęciem nowej operacji tworzenia kopii zapasowej i ustawiono liczbę zachowywanych kopii zapasowych jako zero.

  Ostrzeżenie!
  Jeśli przez takie zastosowanie zasad przechowywania zostanie usunięta jedyna zachowana kopia zapasowa, to w razie niepowodzenia operacji tworzenia kopii zapasowej nie będzie można przywrócić danych, ponieważ nie będzie dostępna żadna kopia zapasowa, z której można by było skorzystać.

- Kopie zapasowe przechowywane na taśmach nie są usuwane, dopóki taśma nie zostanie nadpisana.
- Jeśli zgodnie ze schematem tworzenia kopii zapasowych i formatem kopii zapasowych każda kopia zapasowa jest przechowywana jako oddzielny plik, tego pliku nie można usunąć, dopóki nie upłynie okres przechowywania jej wszystkich zależnych (przyrostowych i różnicowych) kopii zapasowych. Wymagane jest więc dodatkowe miejsce na przechowywanie kopii zapasowych, których usunięcie zostało opóźnione. Ponadto określone wartości mogą zostać przekroczone ze względu na wiek, liczbę lub rozmiar kopii zapasowych.

  To zachowanie można zmienić za pomocą opcji tworzenia kopii zapasowych „Konsolidacja kopii zapasowych”.
- Reguły przechowywania stanowią element planu ochrony. Jeśli plan ochrony zostanie odwołany lub usunięty z komputera albo komputer zostanie usunięty z serwera zarządzania, reguły przestaną działać w odniesieniu do kopii zapasowych tego komputera. Jeśli kopie zapasowe utworzone w ramach danego planu nie są już potrzebne, usuń je zgodnie z opisem podanym w sekcji „Usuwanie kopii zapasowych”.

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 nie da się odzyskać zaszyfrowanych kopii zapasowych.

Szyfrowanie w planie ochrony

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

Aby określić ustawienia szyfrowania w planie ochrony

1. Na panelu planu ochrony 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 jest potrzebne unikatowe hasło dla każdego komputera lub trzeba wymusić szyfrowanie kopii zapasowych niezależnie od ustawień szyfrowania planu ochrony, należy zapisać ustawienia szyfrowania na każdym komputerze z osobna. Kopie zapasowe zostaną zaszyfrowane przy użyciu algorytmu AES z kluczem 256-bitowym.

Zapisanie ustawień szyfrowania na komputerze wpływa na plany ochrony w sposób następujący:

- **Plany ochrony już zastosowane do komputera.** Jeśli ustawienia szyfrowania w planie ochrony są inne, nie uda się utworzyć kopii zapasowych.
- **Plany ochrony, które zostaną zastosowane do komputera później.** Ustawienia szyfrowania zapisane na komputerze zastąpią ustawienia szyfrowania w planie ochrony. Każda kopia zapasowa zostanie zaszyfrowana — nawet jeśli wyłączono szyfrowanie w ustawieniach planu ochrony.

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.

Po zapisaniu ustawień szyfrowania można je zmienić lub zresetować w opisany poniżej sposób.

Ważne
Jeśli już utworzono kopie zapasowe w ramach planu ochrony działającego na tym komputerze, zmiana ustawień szyfrowania spowoduje niepowodzenie wykonania planu. Aby kopie zapasowe były nadal tworzone, utwórz nowy plan.

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, w której został zainstalowany agent ochrony. 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>`

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, w której został zainstalowany agent ochrony. 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**

Aby zmienić ustawienia szyfrowania przy użyciu narzędzia Cyber Protect Monitor

1. Zaloguj się jako administrator w systemie Windows lub macOS.
2. Kliknij ikonę **Cyber Protect Monitor** w obszarze powiadomień (w systemie Windows) lub na pasku menu (w systemie macOS).
3. Kliknij ikonę koła zębatego.
4. Kliknij **Szyfrowanie**.

5. Wykonaj jedną z następujących czynności:
   - Wybierz **Ustaw określone hasło dla tego komputera**. Określ i potwierdź hasło szyfrowania.
   - Wybierz **Użyj ustawień szyfrowania określonych w planie ochrony**.
6. Kliknij **OK**.

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.

Notaryzacja

Notaryzacja pozwala udowodnić, że plik jest autentyczny i niezmieniony od momentu uwzględnienia w kopii zapasowej. Notaryzację warto włączyć w przypadku tworzenia kopii zapasowej plików dokumentów prawnych lub innych plików, które wymagają potwierdzenia autentyczności.

Notaryzacja jest dostępna tylko w przypadku kopii zapasowych na poziomie plików. Pliki z podpisem cyfrowym są pomijane, ponieważ nie trzeba ich notaryzować.

Notaryzacja *nie* jest dostępna w następujących sytuacjach:

- Jeśli format kopii zapasowej jest ustawiony jako **Wersja 11**
- Jeśli lokalizacją docelową kopii zapasowej jest strefa Secure Zone
- Jeśli lokalizacją docelową kopii zapasowej jest lokalizacja zarządzana z włączoną deduplikacją lub szyfrowaniem.

Jak korzystać z funkcji notaryzacji

Aby włączyć notaryzację wszystkich plików wybranych do uwzględnienia w kopii zapasowej (z wyjątkiem plików z podpisem cyfrowym), włącz przełącznik **Notaryzacja** podczas tworzenia planu ochrony.

W ramach konfiguracji odzyskiwania notaryzowane pliki będą oznaczone specjalną ikoną i będzie można zweryfikować ich autentyczność.

Sposób działania

Podczas tworzenia kopii zapasowej agent oblicza kody skrótów uwzględnianych w kopii plików, buduje drzewo skrótów (na podstawie struktury folderów), zapisuje drzewo w kopii zapasowej, a następnie wysyła główne drzewo skrótów do usługi notaryzacji. Usługa notaryzacji zapisuje główne drzewo skrótów w bazie danych łańcucha bloków Ethereum, aby zapewnić, że ta wartość nie zostanie zmieniona.

Weryfikując autentyczność pliku, agent oblicza jego skrót, a następnie porównuje go ze skrótem przechowywanym w drzewie skrótów w kopii zapasowej. W przypadku niezgodności skrótów uznaje się, że plik nie jest autentyczny. W przeciwnym razie autentyczność plików jest gwarantowana przez drzewo skrótów.

Aby zweryfikować, czy samo drzewo skrótów nie zostało naruszone, agent wysyła główne drzewo skrótów do usługi notaryzacji. Usługa notaryzacji porównuje je z drzewem przechowywanym w bazie danych łańcucha bloków. Jeśli skróty są zgodne, wybrany plik otrzymuje gwarancję autentyczności. W przeciwnym razie program wyświetla komunikat, że plik nie jest autentyczny.

Konwersja na maszynę wirtualną

Ważne
Niektóre funkcje opisane w tej sekcji są dostępne tylko w przypadku wdrożeń lokalnych.

Konwersja na maszynę wirtualną jest możliwa tylko dla kopii zapasowych na poziomie dysku. Jeśli kopia zapasowa obejmuje wolumin systemowy i zawiera wszystkie informacje potrzebne do uruchomienia systemu operacyjnego, wynikowa maszyna wirtualna może się uruchomić samodzielnie. W przeciwnym razie jej dyski wirtualne można dodać do innej maszyny wirtualnej.

Metody konwersji

- **Regularna konwersja**
  Konwersję regularną można skonfigurować na dwa sposoby:
  - **Włączenie konwersji w plan ochrony**
    Konwersja zostanie wykonana po każdej operacji tworzenia kopii zapasowej (jeśli jest skonfigurowana w przypadku lokalizacji podstawowej) lub po każdej replikacji (jeśli jest skonfigurowana dla drugiej lokalizacji i następnych).
  - **Utworzenie oddzielnego planu konwersji**
    Ta metoda umożliwia określenie osobnego harmonogramu konwersji.
- **Odzyskanie danych na nową maszynę wirtualną**
  Ta metoda umożliwia wybranie dysków na potrzeby odzyskiwania i dostosowanie ustawień w przypadku każdego dysku wirtualnego. Użyj tej metody do konwersji jednokrotnej lub okazjonalnej, na przykład w celu migracji komputera fizycznego na maszynę wirtualną.

Co trzeba wiedzieć o konwersji

Obsługiwane typy maszyn wirtualnych

Konwersja kopii zapasowej na maszynę wirtualną może zostać wykonana przez tego samego agenta, który utworzył kopię zapasową, lub innego.

Aby dokonać konwersji na maszynę VMware ESXi, Hyper-V lub Scale Computing HC3, potrzebny jest odpowiednio host ESXi, Hyper-V lub Scale Computing HC3 oraz zarządzający nim agent ochrony (agent dla VMware, agent dla Hyper-V lub agent dla Scale Computing HC3).

Konwersja na pliki VHDX jest wykonywana przy założeniu, że pliki zostaną podłączone do maszyny wirtualnej Hyper-V jako dyski wirtualne.

W poniższej tabeli zestawiono typy maszyn wirtualnych, które mogą być tworzone przez agenty:

Typ maszyny wirtualnej	Agent dla VMware	Agent dla Hyper-V	Agent dla systemu Windows	Agent dla systemu Linux	Agent dla systemu Mac	Agent dla Scale Computing HC3
VMware ESXi	+	–	–	–	–	–
Microsoft Hyper-V	–	+	–	–	–	–
VMware Workstation	+	+	+	+	–	–
Pliki VHDX	+	+	+	+	–	–
Scale Computing HC3	–	–	–	–	–	+

Ograniczenia

- Agent dla systemu Windows, agent dla VMware (Windows) ani agent dla Hyper-V nie może konwertować kopii zapasowych przechowywanych w systemie NFS.
- Kopii zapasowych przechowywanych w systemie NFS lub na serwerze SFTP nie można konwertować w ramach osobnego planu konwersji.
- Kopie zapasowe przechowywane na partycji Secure Zone mogą być konwertowane tylko przez agenta działającego na tym samym komputerze.
- Kopie zapasowe można konwertować na maszyny wirtualne Scale Computing HC3 tylko w ramach osobnego planu konwersji.

- Kopie zapasowe zawierające woluminy logiczne systemu Linux (LVM) można konwertować tylko wtedy, gdy zostały utworzone przez agenta dla VMware, agenta dla Hyper-V lub agenta dla Scale Computing HC3 i są kierowane do tego samego hiperwizora. Konwersja między hiperwizorami nie jest obsługiwana.
- W przypadku konwertowania kopii zapasowych komputera z systemem Windows na maszynę wirtualną VMware Workstation lub pliki VHDX wynikowa maszyna wirtualna dziedziczy typ procesora po komputerze dokonującym konwersji. W związku z tym w systemie operacyjnym-gościu są instalowane odpowiednie sterowniki procesora. W przypadku uruchomienia na hoście z procesorem innego typu system-gość wyświetla błąd sterownika. Sterownik należy zaktualizować ręcznie.

Konwersja regularna na maszynę ESXi i Hyper-V a uruchamianie maszyny wirtualnej z kopii zapasowej

Obie operacje zapewniają maszynę wirtualną, którą można uruchomić w czasie liczonym w sekundach, jeśli oryginalna maszyna ulegnie awarii.

Konwersja regularna wykorzystuje zasoby procesora i pamięci. Pliki maszyny wirtualnej stale zajmują miejsce w magazynie danych (pamięci masowej). Jeśli w celu konwersji posłużono się hostem produkcyjnym, może to być niepraktyczne. Wydajność maszyny wirtualnej jednak jest ograniczona tylko przez zasoby hosta.

W drugim przypadku zasoby są wykorzystywane tylko w czasie działania maszyny wirtualnej. Miejsce w magazynie danych (pamięci masowej) jest potrzebne tylko do przechowywania zmian zachodzących na dyskach wirtualnych. Maszyna wirtualna może jednak działać wolniej, ponieważ komputer nie ma bezpośredniego dostępu do dysków wirtualnych, tylko komunikuje się z agentem, który odczytuje dane z kopii zapasowej. Ponadto ta maszyna wirtualna jest tymczasowa.

Konwersja na maszynę wirtualną w planie ochrony

Dostępna jest możliwość skonfigurowania konwersji na maszynę wirtualną z dowolnej lokalizacji kopii zapasowych lub replikacji dostępnej w planie ochrony. Konwersja zostanie przeprowadzona po każdej operacji tworzenia kopii zapasowej lub replikacji.

Informacje na temat wymagań wstępnych i ograniczeń zawiera sekcja „Co trzeba wiedzieć o konwersji”.

Aby skonfigurować konwersję na maszynę wirtualną w planie ochrony

1. Określ lokalizację kopii zapasowej, z której chcesz dokonać konwersji.
2. Na panelu planu ochrony kliknij **Konwertuj na maszynę wirtualną** w obszarze tej lokalizacji.
3. Włącz przełącznik **Konwersja**.
4. W obszarze **Konwertuj na** wybierz typ docelowej maszyny wirtualnej. Można wybrać jedną z następujących opcji:

- **VMware ESXi**
- **Microsoft Hyper-V**
- **VMware Workstation**
- **Pliki VHDX**

5. Wykonaj jedną z następujących czynności:
   - W przypadku maszyn VMware ESXi i Hyper-V: kliknij **Host**, wybierz host docelowy, a następnie określ szablon nazw nowych maszyn.
   - W przypadku maszyn wirtualnych innego typu: w polu **Ścieżka** wskaż miejsce zapisu oraz szablon nazw plików maszyn wirtualnych.

   Domyślna nazwa to **[Nazwa komputera]_skonwertowany**.
6. [Opcjonalnie] Kliknij **Agent, który przeprowadzi konwersję** i wybierz agenta.

   Może to być agent, który wykonuje kopię zapasową (domyślnie), lub agent zainstalowany na innym komputerze. W tym drugim przypadku kopie zapasowe muszą być przechowywane w lokalizacji udostępnionej, np. folderze sieciowym, tak aby ten inny komputer miał do nich dostęp.
7. [Opcjonalnie] W przypadku maszyn VMware ESXi i Hyper-V możesz też zrobić tak:
   - Kliknij **Magazyn danych** w przypadku ESXi lub **Ścieżka** w przypadku Hyper-V, a następnie wybierz magazyn danych (magazyn) dla maszyny wirtualnej.
   - Zmień tryb alokowania dysku. Ustawienie domyślne to **Elastyczne** dla VMware ESXi i **Powiększający się dynamicznie** dla Hyper-V.
   - Kliknij **Ustawienia maszyny wirtualnej**, aby zmienić rozmiar pamięci, liczbę procesorów oraz połączenia sieciowe maszyny wirtualnej.
8. Kliknij **Gotowe**.

Zasada działania zwykłej konwersji na maszynę wirtualną (VM)

Sposób działania konwersji regularnych zależy od wybranego miejsca, w którym ma zostać utworzona maszyna wirtualna.

- **W przypadku wybrania opcji zapisu maszyny wirtualnej w postaci zestawu plików:** każda konwersja powoduje ponowne utworzenie tej maszyny od podstaw.
- **W przypadku wybrania opcji utworzenia maszyny wirtualnej na serwerze wirtualizacji:** w ramach konwersji przyrostowej lub różnicowej kopii zapasowej program nie tworzy ponownie maszyny wirtualnej, tylko aktualizuje maszynę już istniejącą. Taka konwersja trwa zwykle krócej. Wymaga ona przesłania przez sieć mniejszej ilości danych i mniej obciąża procesor hosta wykonującego konwersję. Jeśli aktualizacja maszyny wirtualnej nie jest możliwa, program utworzy ją od podstaw.

Poniżej zamieszczono szczegółowy opis obu tych przypadków.

Po wybraniu opcji zapisu maszyny wirtualnej w postaci zestawu plików

W wyniku pierwszej konwersji tworzona jest nowa maszyna wirtualna. Każda kolejna konwersja powoduje ponowne utworzenie tej maszyny od podstaw. Najpierw tymczasowo zmieniana jest

nazwa starej maszyny. Następnie program tworzy nową maszynę wirtualną o takiej samej nazwie, jak poprzednia nazwa starej maszyny. Jeśli operacja ta zakończy się powodzeniem, program usuwa starą maszynę. Jeśli operacja ta zakończy się niepowodzeniem, program usuwa nową maszynę i przywraca poprzednią nazwę starej maszynie. Oznacza to, że rezultatem konwersji zawsze jest jedna maszyna wirtualna. Jednak podczas konwersji wymagane jest dodatkowe miejsce, tak aby zmieściła się także stara maszyna.

Po wybraniu opcji tworzenia maszyny wirtualnej na serwerze wirtualizacji

Pierwsza konwersja spowoduje utworzenie nowej maszyny wirtualnej. Każda kolejna zadziała zgodnie z następującą zasadą:

- Jeśli od czasu ostatniej konwersji została utworzona *pełna kopia zapasowa*, maszyna wirtualna zostanie ponownie utworzona od podstaw, tak jak opisano wcześniej w tej sekcji.
- W innym przypadku istniejąca maszyna wirtualna zostanie zaktualizowana zgodnie ze zmianami dokonanymi od czasu ostatniej konwersji. Jeśli aktualizacja nie będzie możliwa (na przykład usunięto migawki pośrednie — zobacz poniżej), maszyna wirtualna zostanie utworzona ponownie od podstaw.

Migawki pośrednie

Aktualizacja maszyny wirtualnej wymaga zapisania przez program kilku jej migawek pośrednich. Mają one nazwy zaczynające się od **Backup...** oraz **Replica...** i należy je zachować. Niepotrzebne migawki są usuwane automatyczne.

Najnowsza migawka **Replica...** odpowiada wynikowi ostatniej konwersji. Można z niej skorzystać w celu przywrócenia maszyny do jej ostatniego stanu, na przykład do odrzucenia wprowadzonych zmian po zakończeniu pracy z maszyną.

Pozostałe migawki są przeznaczone do użytku wewnętrznego przez program.

Replikacja

Ważne
Niektóre funkcje opisane w tej sekcji są dostępne tylko w przypadku wdrożeń lokalnych.

W tej sekcji opisano replikację kopii zapasowych w ramach planu ochrony. Aby uzyskać informacje na temat tworzenia oddzielnego planu replikacji, zobacz „Przetwarzanie danych poza hostem”.

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
- Serwer SFTP
- Lokalizacje zarządzane przez węzeł magazynowania

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

- Folder lokalny
- Folder sieciowy
- Chmura
- Serwer SFTP
- Lokalizacje zarządzane przez węzeł magazynowania
- Urządzenie taśmowe

Aby włączyć replikację kopii zapasowych

1. W panelu planu ochrony kliknij **Dodaj lokalizację**.

   Opcja **Dodaj lokalizację** jest dostępna tylko wtedy, gdy replikacja jest obsługiwana *z* ostatniej wybranej lokalizacji kopii zapasowych lub replikacji.
2. Określ lokalizację, w której będą replikowane kopie zapasowe.
3. [Opcjonalnie] W polu **Okres przechowywania** zmień reguły przechowywania dla wybranej lokalizacji zgodnie z instrukcjami podanymi w sekcji „Reguły przechowywania”.
4. [Opcjonalnie] W obszarze **Konwertuj na maszynę wirtualną** określ ustawienia konwersji na maszynę wirtualną zgodnie z instrukcjami podanymi w sekcji „Konwersja na maszynę wirtualną”.

5. [Opcjonalnie] Kliknij ikonę koła zębatego > **Wydajność i okno na utworzenie kopii zapasowej**, a następnie skonfiguruj okno na utworzenie kopii zapasowej dla wybranej lokalizacji, tak jak opisano w sekcji „Wydajność i okno na utworzenie kopii zapasowej”. Te ustawienia decydują o wydajności replikacji.
6. [Opcjonalnie] Powtórz kroki 1–5 w odniesieniu do wszystkich lokalizacji, w których mają być replikowane kopie zapasowe. Obsługiwanych jest maksymalnie pięć kolejnych lokalizacji, wliczając w to podstawową lokalizację.

Ważne
W przypadku włączenia tworzenia kopii zapasowych i replikacji w tym samym planie ochrony należy dopilnować, aby replikacja została zakończona przed uruchomieniem następnej zaplanowanej operacji tworzenia kopii zapasowej. Jeśli replikacja wciąż jest w toku, zaplanowana operacja tworzenia kopii zapasowej nie zostanie uruchomiona. Jeśli więc na przykład replikacja potrwa 26 godzin, to zaplanowana operacja tworzenia kopii zapasowej uruchamiana co 24 godziny nie zostanie rozpoczęta.

Aby uniknąć takiej zależności, należy zastosować osobny plan na potrzeby replikacji kopii zapasowych. Więcej informacji na temat tego konkretnego planu można znaleźć w sekcji "Replikacja kopii zapasowej" (s. 364).

Uwagi dla użytkowników mających licencję zaawansowaną

Wskazówka

Replikację kopii zapasowych możesz skonfigurować *z* magazynu chmurowego, tworząc oddzielny plan replikacji. Aby uzyskać więcej informacji, zobacz „Przetwarzanie danych poza hostem”.

Ograniczenia

- Replikacja kopii zapasowych *z* lokalizacji zarządzanej przez węzeł magazynowania do folderu lokalnego nie jest obsługiwana. Folder lokalny to folder na komputerze zawierającym agenta, który utworzył kopię zapasową.
- Replikacja kopii zapasowych *do* lokalizacji zarządzanej z włączoną deduplikacją nie jest obsługiwana dla kopii zapasowych mających format kopii zapasowej **Wersja 12**.

Na którym komputerze jest wykonywana operacja?

Replikowanie kopii zapasowej *z* dowolnej lokalizacji jest inicjowane przez agenta, który utworzył kopię zapasową. Operację tę wykonuje:

- Ten agent, jeśli lokalizacja *nie jest* zarządzana przez węzeł magazynowania.
- Odpowiedni węzeł magazynowania, jeśli lokalizacja jest zarządzana. Jednak replikacja kopii zapasowej z lokalizacji zarządzanej do magazynu chmurowego jest wykonywana przez agenta, który utworzył kopię zapasową.

Jak wynika z powyższego opisu, operacja ta zostanie przeprowadzona jedynie wtedy, gdy komputer z agentem jest włączony.

Replikacja kopii zapasowych między lokalizacjami zarządzanymi

Replikowanie kopii zapasowej z jednej lokalizacji zarządzanej do innej lokalizacji zarządzanej jest realizowane przez węzeł magazynowania.

Jeśli dla lokalizacji docelowej jest włączona deduplikacja (być może w innym węźle magazynowania), źródłowy węzeł magazynowania wysyła tylko te bloki danych, których nie ma w lokalizacji docelowej. Inaczej mówiąc, węzeł magazynowania, podobnie jak agent, wykonuje deduplikację w źródle. Pozwala ta zmniejszyć ruch sieciowy w przypadku replikowania danych między węzłami magazynowania w różnych lokalizacjach geograficznych.

Ręczne rozpoczynanie tworzenia kopii zapasowych

1. Wybierz komputer z co najmniej jednym stosowanym planem ochrony.
2. Kliknij **Kopia zapasowa**.
3. Jeśli jest stosowany więcej niż jeden plan ochrony, wybierz odpowiedni plan.
4. Wykonaj jedną z następujących czynności:
   - Kliknij **Uruchom teraz**. Zostanie utworzona przyrostowa kopia zapasowa.
   - Jeśli schemat tworzenia kopii zapasowych obejmuje kilka metod tworzenia kopii zapasowych, można wybrać metodę, która ma zostać użyta. Kliknij strzałkę na przycisku **Uruchom teraz** i wybierz opcję **Pełna, Przyrostowa** lub **Różnicowa**.

Pierwsza kopia zapasowa utworzona w ramach planu ochrony jest zawsze pełna.

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

Opcje tworzenia kopii zapasowych

Ważne
Niektóre funkcje opisane w tej sekcji są dostępne tylko w przypadku wdrożeń lokalnych.

Aby zmienić opcje tworzenia kopii zapasowych, kliknij ikonę koła zębatego widoczną obok nazwy planu ochrony, 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, macOS).
- 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	macOS	Windows	Linux	macOS	ESXi	Hyper-V	Scale Computing	Windows
Alerty	+	+	+	+	+	+	+	+	+	+
Konsolidacja kopii zapasowych	+	+	+	+	+	+	+	+	+	-
Nazwa pliku kopii zapasowej	+	+	+	+	+	+	+	+	+	+
Format kopii zapasowej	+	+	+	+	+	+	+	+	+	+
Sprawdzanie poprawności kopii zapasowej	+	+	+	+	+	+	+	+	+	+
CBT (Changed Block Tracking)	+	-	-	-	-	-	+	+	+	+
Tryb tworzenia kopii zapasowych klastra	-	-	-	-	-	-	-	-	-	+
Stopień kompresji	+	+	+	+	+	+	+	+	+	+
Powiadomienia e-mail	+	+	+	+	+	+	+	+	+	+
Obsługa błędów										
W przypadku wystąpienia błędu spróbuj ponownie	+	+	+	+	+	+	+	+	+	+

Nie pokazuj komunikatów ani okien dialogowych podczas przetwarzania (tryb cichy)	+	+	+	+	+	+	+	+	+	+
Ignoruj uszkodzone sektory	+	-	+	+	-	+	+	+	+	-
W razie błędu tworzenia migawki maszyny wirtualnej spróbuj ponownie	-	-	-	-	-	-	+	+	+	-
Szybka przyrostowa/różnicowa kopia zapasowa	+	+	+	-	-	-	-	-	-	-
Filtry plików	+	+	+	+	+	+	+	+	+	-
Migawka kopii zapasowej na poziomie plików	-	-	-	+	+	+	-	-	-	-
Obcinanie dziennika	-	-	-	-	-	-	+	+	-	Tylko SQL
Wykonywanie migawek LVM	-	+	-	-	-	-	-	-	-	-
Punkty zamontowania	-	-	-	+	-	-	-	-	-	-
Migawka wielowolumino wa	+	+	-	+	+	-	-	-	-	-
Wydajność i okno na utworzenie	+	+	+	+	+	+	+	+	+	+

kopii zapasowej										
Fizyczne dostarczanie danych	+	+	+	+	+	+	+	+	+	-
Polecenia poprzedzające/ następujące	+	+	+	+	+	+	+	+	+	+
Polecenia poprzedzające rejestrowanie danych/następujące po nim	+	+	+	+	+	+	+	-	-	+
Migawki urządzenia SAN	-	-	-	-	-	-	+	-	-	-
Tworzenie harmonogramu										
Rozłóż uruchamianie w przedziale czasu	+	+	+	+	+	+	+	+	+	+
Ogranicz liczbę jednoczesnych operacji tworzenia kopii zapasowych	-	-	-	-	-	-	+	+	+	-
Kopia zapasowa sektor po sektorze	+	+	-	-	-	-	+	+	+	-
Dzielenie	+	+	+	+	+	+	+	+	+	+
Zarządzanie taśmami	+	+	+	+	+	+	+	+	+	+
Obsługa niepowodzenia zadania	+	+	+	+	+	+	+	+	+	+

Warunki uruchomienia zadania	+	+	-	+	+	-	+	+	+	+
Usługa kopiowania woluminów w tle (VSS)	+	-	-	+	-	-	-	+	-	+
Usługa kopiowania woluminów w tle (VSS) dla maszyn wirtualnych	-	-	-	-	-	-	+	+	+	-
Tygodniowa kopia zapasowa	+	+	+	+	+	+	+	+	+	+
Dziennik zdarzeń systemu Windows	+	-	-	+	-	-	+	+	+	+

Alerty

Brak pomyślnie utworzonych kopii zapasowych przez określoną liczbę kolejnych dni

Ustawienie wstępne: **Wyłączono**.

Ta opcja pozwala określić, czy oprogramowanie ma wygenerować alert, jeśli przez określony czas w ramach planu ochrony nie zostanie utworzona pomyślnie ani jedna kopia zapasowa. Oprócz nieudanych operacji tworzenia kopii zapasowych oprogramowanie zlicza kopie zapasowe, które nie zostały uruchomione zgodnie z harmonogramem (pominięte kopie zapasowe).

Alerty są generowane dla poszczególnych komputerów i wyświetlane na karcie **Alerty**.

Można określić liczbę dni bez kopii zapasowej, po których jest generowany alert.

Konsolidacja kopii zapasowych

Ta opcja określa, czy konsolidować kopie zapasowe podczas czyszczenia, czy też usuwać całe ciągi kopii zapasowych.

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 jedynie metoda usuwania, ale 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.

Ta opcja *nie* jest skuteczna, jeśli występuje co najmniej jedna z następujących sytuacji:

- Miejscem docelowym kopii zapasowej jest urządzenie taśmowe lub magazyn chmurowy.
- Schemat tworzenia kopii zapasowych jest ustawiony jako **Zawsze przyrostowa (jednoplikowa)**.
- Format kopii zapasowej jest ustawiony jako **Wersja 12**.

Kopii zapasowych przechowywanych na taśmach nie można konsolidować. Kopie zapasowe przechowywane w magazynie chmurowym oraz jednoplikowe kopie zapasowe w wersji 11 i 12 są zawsze konsolidowane, ponieważ ich struktura wewnętrzna umożliwia szybką i łatwą konsolidację.

Jednak w przypadku korzystania z wersji 12 oraz obecności wielu ciągów kopii zapasowych (każdy ciąg zapisywany w osobnym pliku .tibx) konsolidacja działa tylko w obrębie ostatniego ciągu. Wszystkie pozostałe ciągi są całkowicie usuwane – za wyjątkiem pierwszego, który jest pomniejszany do minimalnego rozmiaru pozwalającego na zachowanie metainformacji (około 12 KB). Te metainformacje są niezbędne do zapewnienia spójności danych podczas jednoczesnych operacji odczytu i zapisu. Zawarte w tych ciągach kopie zapasowe znikają z graficznego interfejsu użytkownika natychmiast po zastosowaniu reguły przechowywania, choć nadal istnieją fizycznie aż do usunięcia całego ciągu.

We wszystkich pozostałych przypadkach kopie zapasowe, których usunięcie zostanie wstrzymane, będą oznaczone w interfejsie graficznym ikoną kosza na śmieci ( ) Po usunięciu takiej kopii zapasowej poprzez kliknięcie symbolu X zostanie przeprowadzona konsolidacja. Kopie zapasowe przechowywane na taśmie znikają z interfejsu użytkownika tylko w razie nadpisania lub usunięcia zawartości taśmy.

Nazwa pliku kopii zapasowej

Ta opcja określa nazwy plików kopii zapasowych tworzonych w ramach planu ochrony.

Te nazwy można zobaczyć w menedżerze plików podczas przeglądania lokalizacji kopii zapasowej.

Co to jest plik kopii zapasowej?

W ramach każdego planu ochrony w lokalizacji kopii zapasowych jest tworzony co najmniej jeden plik — w zależności od używanego schematu tworzenia kopii zapasowych i formatu kopii zapasowych. Poniższa tabela zawiera pliki, które można utworzyć dla komputera lub skrzynki pocztowej.

	Zawsze przyrostowa (jednoplikowa)	**Inne schematy tworzenia kopii zapasowych**
Format kopii zapasowej **Wersja 11**	Jeden plik TIB i jeden plik metadanych XML	Wiele plików TIB i jeden plik metadanych XML (tradycyjny format)
Format kopii zapasowej **Wersja 12**	Jeden plik TIBX na ciąg kopii zapasowych (pełna lub różnicowa kopia zapasowa oraz wszystkie przyrostowe kopie zapasowe, które od niej zależą)	

Wszystkie pliki mają taką samą nazwę z dodaną sygnaturą czasową lub numerem sekwencyjnym lub bez. Tę nazwę (określaną jako nazwa pliku kopii zapasowej) można określić podczas tworzenia lub edytowania planu ochrony.

Uwaga
Sygnatura czasowa jest dodawana do nazwy pliku kopii zapasowej tylko w przypadku formatu w wersji 11.

Po zmianie nazwy pliku kopii zapasowej kolejna kopia zapasowa będzie pełną kopią zapasową, chyba że określisz nazwę pliku istniejącej kopii zapasowej na tym samym komputerze. W tym drugim przypadku zostanie utworzona pełna, przyrostowa lub różnicowa kopia zapasowa — zgodnie z harmonogramem planu ochrony.

Pamiętaj, że można ustawić nazwy plików kopii zapasowej dla lokalizacji, których nie można przeglądać za pomocą menedżera plików (takich jak magazyn chmurowy lub urządzenie taśmowe). Warto to zrobić, jeśli na karcie **Magazyn kopii zapasowych** mają być wyświetlane niestandardowe nazwy.

Gdzie mogę zobaczyć nazwy plików kopii zapasowej?

Wybierz kartę **Magazyn kopii zapasowych**, a następnie wybierz grupę kopii zapasowych.

- Domyślna nazwa pliku kopii zapasowej jest pokazywana na panelu **Szczegóły**.
- Jeśli ustawisz inną nazwę pliku kopii zapasowej niż domyślna, będzie ona bezpośrednio widoczna na karcie **Magazyn kopii zapasowych** w kolumnie **Nazwa**.

Ograniczenia nazw plików kopii zapasowej

- Nazwa pliku kopii zapasowej nie może kończyć się cyfrą.

  W domyślnej nazwie pliku kopii zapasowej, aby uniknąć kończenia nazwy cyfrą, dołączana jest litera „A”. Podczas tworzenia nazwy niestandardowej zawsze się upewnij, że nie kończy się ona cyfrą. W przypadku używania zmiennych nazwa pliku kopii zapasowej nie może się kończyć zmienną, ponieważ zmienna może kończyć się cyfrą.
- Nazwa pliku kopii zapasowej nie może zawierać następujących symboli: **()&?*$<>":\|/#**, znaków końca wiersza (**\n**) ani znaków tabulacji (**\t**).

Domyślna nazwa pliku kopii zapasowej

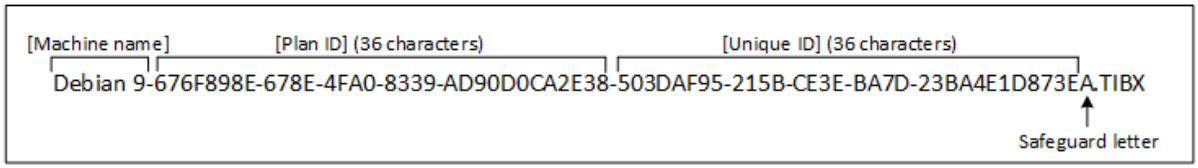
Domyślna nazwa pliku kopii zapasowej to `[Nazwa komputera]-[Identyfikator planu]-[Unikatowy identyfikator]A`.

Domyślna nazwa pliku kopii zapasowej dla kopii zapasowej skrzynki pocztowej to `[Identyfikator skrzynki pocztowej]_mailbox_[Identyfikator planu]A`.

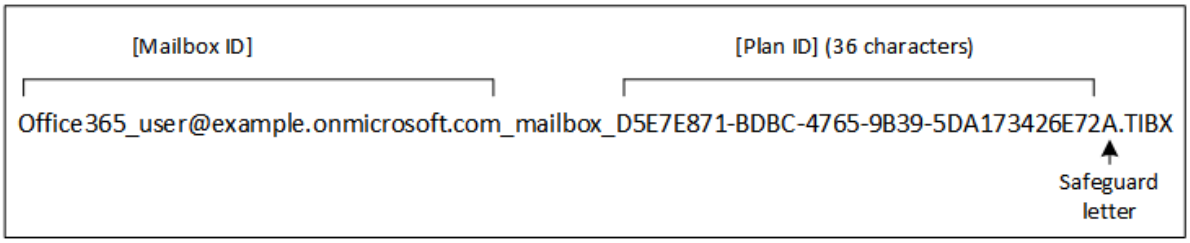
Nazwa składa się z następujących zmiennych:

- `[Nazwa komputera]` Ta zmienna jest zastępowana przez nazwę komputera (tę samą, która jest widoczna w konsoli internetowej Cyber Protect) w przypadku wszystkich typów danych zawartych w kopii zapasowej, z wyjątkiem skrzynek pocztowych Microsoft 365. W przypadku skrzynek pocztowych Microsoft 365 jest ona zastępowana przez główną nazwę użytkownika (UPN) skrzynki pocztowej.
- `[Identyfikator planu]` Ta zmienna jest zastępowana przez unikatowy identyfikator planu ochrony. Ta wartość się nie zmienia przy zmianie nazwy planu.
- `[Unikatowy identyfikator]` Ta zmienna jest zastępowana przez unikatowy identyfikator wybranego komputera lub skrzynki pocztowej. Ta wartość się nie zmienia przy zmianie nazwy komputera lub zmianie UPN skrzynki pocztowej.
- `[Identyfikator skrzynki pocztowej]` Ta zmienna jest zastępowana przez UPN skrzynki pocztowej.
- „`A`” to litera zabezpieczająca dołączana, aby uniknąć kończenia nazwy cyfrą.

Poniższy diagram pokazuje domyślną nazwę pliku kopii zapasowej.



Poniższy diagram pokazuje domyślną nazwę pliku kopii zapasowej dla skrzynek pocztowych.



Nazwy bez zmiennych

Jeśli zmienisz nazwę pliku kopii zapasowej na `Moja_kopia_zapasowa`, pliki kopii zapasowej będą wyglądały podobnie do poniższych przykładów. Oba przykłady zakładają codzienne przyrostowe kopie zapasowe zaplanowane na 14:40, poczynając od 13 września 2016 r.

W przypadku formatu w wersji 12 ze schematem tworzenia kopii zapasowych **Zawsze przyrostowa (jednoplikowa)**:

```
MyBackup.tibx
```

W przypadku formatu w wersji 12 z innymi schematami tworzenia kopii zapasowych:

```
MyBackup.tibx
MyBackup-0001.tibx
MyBackup-0002.tibx
...
```

W przypadku formatu w wersji 11 ze schematem tworzenia kopii zapasowych **Zawsze przyrostowa (jednoplikowa)**:

```
MyBackup.xml
MyBackup.tib
```

W przypadku formatu w wersji 11 z innymi schematami tworzenia kopii zapasowych:

```
MyBackup.xml
MyBackup_2016_9_13_14_49_20_403F.tib
MyBackup_2016_9_14_14_43_00_221F.tib
MyBackup_2016_9_15_14_45_56_300F.tib
...
```

Używanie zmiennych

Oprócz zmiennych, które są używane domyślnie, możesz użyć zmiennej `[Nazwa planu]`, która jest zastępowana przez nazwę planu ochrony.

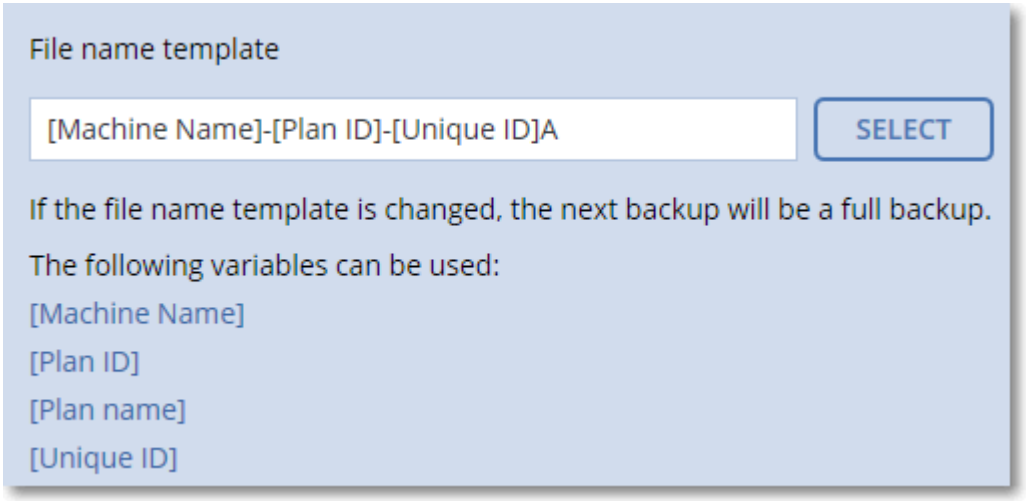
Jeśli do kopii zapasowej wybrano wiele komputerów lub skrzynek pocztowych, nazwa pliku kopii zapasowej musi zawierać zmienną `[Nazwa komputera]`, `[Identyfikator skrzynki pocztowej]` lub `[Unikatowy identyfikator]`.

Nazwa pliku kopii zapasowej a uproszczone nazewnictwo plików

Przy użyciu zwykłego tekstu i/lub zmiennych możesz utworzyć takie same nazwy plików, co we wcześniejszych wersjach programu Acronis Cyber Protect. Jednak w wersji 12 nie można zrekonstruować uproszczonych nazw plików — nazwa pliku będzie miała sygnaturę czasową, chyba że jest używany format jednoplikowy.

Przykłady użycia

- **Wyświetl nazwy plików przyjazne dla użytkownika**
  Chcesz łatwo rozróżniać kopie zapasowe podczas przeglądania lokalizacji kopii zapasowej za pomocą menedżera plików.
- **Kontynuuj istniejącą sekwencję kopii zapasowych**
  Załóżmy, że plan ochrony jest stosowany do jednego komputera i że masz usunąć ten komputer z konsoli internetowej Cyber Protect lub odinstalować agenta wraz z jego ustawieniami konfiguracji. Po ponownym dodaniu komputera lub ponownej instalacji agenta możesz wymusić, aby plan ochrony kontynuował tworzenie kopii zapasowej w tej samej kopii zapasowej lub sekwencji kopii zapasowych. W tym celu w sekcji opcji tworzenia kopii zapasowych planu ochrony kliknij **Nazwa pliku kopii zapasowej**, a następnie kliknij **Wybierz**, aby wybrać odpowiednią kopię zapasową.
  Przycisk **Przeglądaj** pozwala wyświetlić kopie zapasowe w lokalizacji wybranej w sekcji **Miejsce docelowe kopii zapasowej** panelu planu ochrony. Nie pozwala on przeglądać niczego poza tą lokalizacją.



- **Uaktualnij z wcześniejszych wersji produktu**
  Jeśli podczas uaktualniania plan ochrony nie został automatycznie objęty migracją, ponownie utwórz plan, wskazując stary plik kopii zapasowej. Jeśli do tworzenia kopii zapasowej został wybrany tylko jeden komputer, kliknij **Przeglądaj**, a następnie wybierz żądaną kopię zapasową. Jeśli do tworzenia kopii zapasowej zostało wybranych wiele komputerów, odtwórz starą nazwę pliku kopii zapasowej przy użyciu zmiennych.

Uwaga
Przycisk **Wybierz** jest dostępny tylko w przypadku planów ochrony tworzonych i stosowanych na potrzeby jednego urządzenia.

Format kopii zapasowej

Ta opcja określa format kopii zapasowych tworzonych w ramach danego planu ochrony. Jest ona dostępna tylko w przypadku planów ochrony korzystających ze starszego formatu kopii zapasowej w wersji 11. W takim przypadku można go zmienić na nowy format w wersji 12. Po takiej zmianie ta opcja przestanie być dostępna.

Ta opcja *nie* jest dostępna w przypadku kopii zapasowych skrzynek pocztowych. Kopie zapasowe skrzynek pocztowych zawsze mają nowy format.

Ustawienie wstępne: **Wybór automatyczny**.

Można wybrać jedną z następujących opcji:

- **Wybór automatyczny**
  Będzie używana Wersja 12, chyba że plan ochrony dołącza kopie zapasowe do kopii utworzonych przy użyciu starszej wersji programu.
- **Wersja 12**
  W większości przypadków najlepiej jest stosować nowy format, który pozwala na szybkie tworzenie kopii zapasowych i odzyskiwanie. Każdy ciąg kopii zapasowych (pełna lub różnicowa kopia zapasowa oraz wszystkie przyrostowe kopie zapasowe, które od niej zależą) jest zapisywany w jednym pliku TIBX.
  Do tego formatu reguła przechowywania **Według łącznego rozmiaru kopii zapasowych** jest nieskuteczna.
- **Wersja 11**
  Starszy format zostanie zachowany w celu zapewnienia kompatybilności wstecz. Umożliwia on dołączanie kopii zapasowych do kopii utworzonych przy użyciu starszej wersji programu.
  Format ten należy stosować [w połączeniu z każdym schematem tworzenia kopii zapasowych z wyjątkiem schematu **Zawsze przyrostowa (jednoplikowa)**] także wtedy, gdy pełne, przyrostowe lub różnicowe kopie zapasowe mają być osobnymi plikami.
  Ten format jest wybierany automatycznie, jeśli miejscem docelowym kopii zapasowej (lub replikacji) jest lokalizacja zarządzana z włączoną deduplikacją lub z włączonym szyfrowaniem. Jeśli zmienisz format na **Wersja 12**, tworzenie kopii zapasowych zakończy się niepowodzeniem.

  Uwaga
  Nie można tworzyć kopii zapasowych grup dostępności bazy danych (Database Availability Group, DAG) przy użyciu formatu kopii zapasowych w wersji 11. Tworzenie kopii zapasowych grup DAG jest obsługiwane tylko w formacie kopii zapasowych w wersji 12.

Format kopii zapasowej i pliki kopii zapasowej

W przypadku lokalizacji kopii zapasowej, które można przeglądać za pomocą menedżera plików (takich jak foldery lokalne lub sieciowe), format kopii zapasowej określa liczbę plików i ich rozszerzenia. Przy użyciu opcji nazwa pliku kopii zapasowej możesz określić nazwy plików. Poniższa tabela zawiera pliki, które można utworzyć dla komputera lub skrzynki pocztowej.

	Zawsze przyrostowa (jednoplikowa)	**Inne schematy tworzenia kopii zapasowych**
Format kopii zapasowej **Wersja 11**	Jeden plik TIB i jeden plik metadanych XML	Wiele plików TIB i jeden plik metadanych XML (tradycyjny format)
Format kopii zapasowej **Wersja 12**	Jeden plik TIBX na ciąg kopii zapasowych (pełna lub różnicowa kopia zapasowa oraz wszystkie przyrostowe kopie zapasowe, które od niej zależą)	

Zmienianie formatu kopii zapasowych na wersję 12 (TIBX)

Jeśli zmienisz format kopii zapasowych z wersji 11 (format TIB) na wersję 12 (format TIBX):

- Następna kopia zapasowa będzie pełna.
- W lokalizacjach kopii zapasowych, które można przeglądać za pomocą menedżera plików (takich jak foldery lokalne lub sieciowe), zostanie utworzony nowy plik TIBX. Nowy plik będzie mieć taką samą nazwę jak oryginalny plik oraz sufiks **_v12A**.
- Reguły przechowywania i replikacja będą stosowane tylko w przypadku nowych kopii zapasowych.
- Stare kopie zapasowe nie zostaną usunięte i nadal będą dostępne na karcie **Magazyn kopii zapasowych**.Można je usunąć ręcznie.
- Stare chmurowe kopie zapasowe nie będą wykorzystywać limitu **Chmura**.
- Stare lokalne kopie zapasowe będą wykorzystywać limit **Lokalna kopia zapasowa**, dopóki nie zostaną usunięte ręcznie.
- Jeśli miejscem docelowym kopii zapasowej (lub replikacji) jest lokalizacja zarządzana z włączoną deduplikacją, operacja tworzenia kopii zapasowej się nie powiedzie.

Deduplikacja w archiwum

W przypadku formatu Wersji 12 obsługiwana jest deduplikacja w archiwum.

Deduplikacja w archiwum stosuje deduplikację po stronie klienta i zapewnia następujące korzyści:

- Znacznie mniejszy rozmiar kopii zapasowych dzięki wbudowanej deduplikacji na poziomie bloków w przypadku każdego rodzaju danych

- Sprawna obsługa twardych łączy, która zapewnia wyeliminowanie duplikatów w magazynach
- Dzielenie na fragmenty na podstawie skrótów

Uwaga
Deduplikacja w archiwum jest domyślnie włączona w przypadku wszystkich kopii zapasowych w formacie TIBX. Nie trzeba jej włączać w opcjach tworzenia kopii zapasowych i nie można jej wyłączyć.

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 ochrony jest od razu sprawdzana pod kątem poprawności. Ta operacja jest wykonywana przez agenta ochrony.

Ustawienie wstępne: **Wyłączono**.

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.

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 w środowisku ESXi bądź Hyper-V.

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. Działa również w przypadku kopii zapasowych baz danych programów Microsoft SQL Server i Microsoft Exchange Server.

Ustawienie wstępne: **Włączono**.

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 dysków lub baz danych są stale monitorowane na poziomie bloków. Po rozpoczęciu tworzenia kopii zapasowej zmiany mogą zostać niezwłocznie zapisane w kopii zapasowej.

Tryb tworzenia kopii zapasowych klastra

Opcje te działają w przypadku kopii zapasowych na poziomie bazy danych programów Microsoft SQL Server i Microsoft Exchange Server.

Działają tylko wtedy, gdy do tworzenia kopii zapasowej został wybrany sam klaster [zawsze włączone grupy dostępności (AAG) programu Microsoft SQL Server lub grupa dostępności bazy danych (DAG) programu Microsoft Exchange Server], a nie poszczególne węzły lub znajdujące się w nich bazy danych. Jeśli wybierzesz poszczególne elementy wewnątrz klastra, kopia zapasowa nie będzie obsługiwać klastra i zostanie utworzona kopia zapasowa tylko wybranych kopii elementów.

Microsoft SQL Server

Ta opcja określa tryb kopii zapasowej dla zawsze włączonych grup dostępności (AAG) programu SQL Server. Aby ta opcja działała, agent dla SQL musi być zainstalowany na wszystkich węzłach zawsze włączonej grupy dostępności (AAG). Więcej informacji o tworzeniu kopii zapasowych zawsze włączonych grup dostępności, zobacz „Ochrona zawsze włączonych grup dostępności (AAG)”.

Ustawienie wstępne: **Replika pomocnicza, jeśli to możliwe.**

Możesz wybrać jedną z poniższych opcji:

- **Replika pomocnicza, jeśli to możliwe**
  Jeśli wszystkie repliki pomocnicze są w trybie offline, jest tworzona kopia zapasowa repliki podstawowej. Tworzenie kopii zapasowej repliki podstawowej może spowolnić działanie programu SQL Server, ale kopia zapasowa zostanie utworzona dla najbardziej aktualnego stanu danych.
- **Replika pomocnicza**
  Jeśli wszystkie repliki pomocnicze są w trybie offline, operacja tworzenia kopii zapasowej się nie powiedzie. Tworzenie kopii zapasowych replik pomocniczych nie wpływa na wydajność serwera SQL i umożliwia wydłużenie okna na utworzenie kopii zapasowej. Jednak pasywne repliki mogą zawierać nieaktualne informacje, ponieważ często są one aktualizowane asynchronicznie (z opóźnieniem).
- **Replika podstawowa**
  Jeśli replika podstawowa jest w trybie offline, operacja tworzenia kopii zapasowej się nie powiedzie. Tworzenie kopii zapasowej repliki podstawowej może spowolnić działanie programu SQL Server, ale kopia zapasowa zostanie utworzona dla najbardziej aktualnego stanu danych.

Bez względu na wartość tej opcji oprogramowanie, aby zapewnić spójność bazy danych, pomija bazy danych, które *nie* są w stanie **SYNCHRONIZED** lub **SYNCHRONIZING**, gdy rozpoczyna się tworzenie kopii zapasowej. Jeśli wszystkie bazy danych zostaną pominięte, operacja tworzenia kopii zapasowej się nie powiedzie.

Microsoft Exchange Server

Ta opcja określa tryb kopii zapasowej dla grup dostępności bazy danych (DAG) programu Exchange Server. Aby ta opcja działała, agent dla programu Exchange musi być zainstalowany na wszystkich węzłach grupy dostępności bazy danych (DAG). Więcej informacji o tworzeniu kopii zapasowych grup dostępności bazy danych, zobacz „Ochrona grup dostępności bazy danych (DAG)”.

Ustawienie wstępne: **Kopia pasywna, jeśli to możliwe.**

Możesz wybrać jedną z poniższych opcji:

- **Kopia pasywna, jeśli to możliwe**
  Jeśli wszystkie kopie pasywne są w trybie offline, jest tworzona kopia zapasowa kopii aktywnej. Tworzenie kopii zapasowej kopii aktywnej może spowolnić działanie programu Exchange Server, ale kopia zapasowa zostanie utworzona dla najbardziej aktualnego stanu danych.
- **Kopia pasywna**
  Jeśli wszystkie kopie pasywne są w trybie offline, operacja tworzenia kopii zapasowej się nie powiedzie. Tworzenie kopii zapasowych kopii pasywnych nie wpływa na wydajność serwera programu Exchange i umożliwia wydłużenie okna na utworzenie kopii zapasowej. Pasywne kopie mogą jednak zawierać nieaktualne informacje, ponieważ często są one aktualizowane asynchronicznie (z opóźnieniem).
- **Kopia aktywna**
  Jeśli kopia aktywna jest w trybie offline, operacja tworzenia kopii zapasowej się nie powiedzie. Tworzenie kopii zapasowej kopii aktywnej może spowolnić działanie programu Exchange Server, ale kopia zapasowa zostanie utworzona dla najbardziej aktualnego stanu danych.

Bez względu na wartość tej opcji oprogramowanie, aby zapewnić spójność bazy danych, pomija bazy danych, które *nie* są w stanie **HEALTHY** lub **ACTIVE**, gdy rozpoczyna się tworzenie kopii zapasowej. Jeśli wszystkie bazy danych zostaną pominięte, operacja tworzenia kopii zapasowej się nie powiedzie.

Stopień kompresji

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

Ustawienie wstępne: **Normalny**.

Wyższy poziom kompresji powoduje, że utworzenie kopii zapasowej trwa dłużej, ale wynikowa kopia zapasowa zajmuje mniej miejsca. Obecnie ustawienia poziomów Wysoki i Maksymalny działają podobnie.

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.

Powiadomienia e-mail

Ta opcja umożliwia skonfigurowanie powiadomień e-mail o zdarzeniach, które wystąpiły podczas wykonywania kopii zapasowych.

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

Ustawienie wstępne: **Użyj ustawień systemu.**

Możesz użyć ustawień systemu albo zastąpić je wartościami niestandardowymi stosowanymi tylko w odniesieniu do tego planu. Ustawienia systemu są konfigurowane zgodnie z opisem podanym w sekcji „Powiadomienia e-mail”.

Ważne
Zmiana ustawień systemu wpłynie na wszystkie korzystające z nich plany ochrony.

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

Aby dostosować powiadomienia e-mail dotyczące planu ochrony

1. Zaznacz **Dostosuj ustawienia na potrzeby tego planu ochrony**.
2. W polu **Adresy e-mail odbiorców** wpisz docelowy adres e-mail. Możesz wprowadzić kilka adresów oddzielonych średnikami.
3. [Opcjonalnie] W polu **Temat** zmień temat powiadomienia pocztą e-mail.
   Możesz użyć następujących zmiennych:
   - `[Alert]` — podsumowanie alertu.
   - `[Urządzenie]` — nazwa urządzenia.
   - `[Plan]` — nazwa planu, który wygenerował alert.
   - `[Serwer zarządzania]` — nazwa hosta komputera, na którym jest zainstalowany serwer zarządzania.
   - `[Jednostka]` — nazwa jednostki, do której należy komputer.

   Domyślnym tematem jest `[Alert]` **Urządzenie:** `[Urządzenie]` **Plan:** `[Plan]`
4. Zaznacz pola wyboru odpowiadające zdarzeniom, o których chcesz otrzymywać powiadomienia. Możesz wybrać z listy wszystkich alertów, które wystąpiły podczas tworzenia kopii zapasowej, zgrupowanych według wagi.

Obsługa błędów

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

W razie błędu spróbuj ponownie

Ustawienie wstępne: **Włączono. 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.

Chmura

W przypadku wybrania chmury jako lokalizacji docelowej kopii zapasowej opcja ta ma automatycznie ustawianą wartość **Włączono**. **Liczba prób: 300**. **Odstęp między próbami: 30 s.**

W tym przypadku nie ma faktycznego limitu liczby prób, ale limit czasu przed niepowodzeniem utworzenia kopii zapasowej jest obliczany w następujący sposób: (300 sekund + **odstęp między próbami**) * (**liczba prób** + 1).

Przykłady:

- Przy domyślnych wartościach tworzenie kopii zapasowej nie powiedzie się po (300 s. + 30 s.) * (300 + 1) = 99 330 sekundach, czyli około 27,6 godziny.
- W przypadku ustawienia **liczby prób** na 1 oraz **odstępu między próbami** na 1 sekundę tworzenie kopii zapasowej nie powiedzie się po (300 s. + 1 s.) * (1 + 1) = 602 sekundach, czyli około 10 minutach.

Jeśli limit czasu przekroczy 30 minut, a transfer danych jeszcze się nie rozpoczął, faktyczny limit jest ustawiany na 30 minut.

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

Ustawienie wstępne: **Włączono**.

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: **Wyłączono**.

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

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: **Włączono. 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.

Szybka przyrostowa/różnicowa kopia zapasowa

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

Ta opcja nie działa (jest zawsze wyłączona) w przypadku woluminów sformatowanych w systemach plików JFS, ReiserFS3, ReiserFS4, ReFS lub XFS.

Ustawienie wstępne: **Włączono**.

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.

Filtry plików

Za pomocą filtrów plików można uwzględnić w kopii zapasowej lub wykluczyć z niej tylko określone pliki i foldery.

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

Filtry plików nie działają w przypadku zastosowania dysków dynamicznych (woluminy LVM lub LDM) w maszynie wirtualnej, której kopia zapasowa wykonywana jest przez agenta dla VMware, agenta dla Hyper-V lub agenta dla Scale Computing w trybie bezagentowym.

Aby włączyć filtry plików

1. W planie ochrony rozwiń moduł **Kopia zapasowa**.
2. W sekcji **Opcje tworzenia kopii zapasowych** kliknij **Zmień**.
3. Wybierz **Filtry plików**.
4. Użyj dowolnych z niżej opisanych opcji.

Uwzględnij lub 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
  Jeśli w polu **Format kopii zapasowej** zostanie wybrana opcja **Wersja 11** i lokalizacją docelową kopii zapasowej NIE jest chmura, ten filtr nie zadziała w przypadku kopii zapasowej na poziomie plików.

- **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.

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 do pliku lub folderu, zaczynając od litery dysku (w przypadku tworzenia kopii zapasowych danych systemu Windows) lub katalogu głównego (w przypadku tworzenia kopii zapasowych systemu Linux lub macOS).
  Zarówno w systemie Windows, jak i Linux/macOS 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**).

Ważne
Jeśli podczas tworzenia kopii zapasowej na poziomie dysku system operacyjny uwzględnianego w kopii komputera nie zostanie poprawnie wykryty, filtry plików oparte na pełnych ścieżkach nie będą działać. W przypadku filtru wykluczającego pojawi się ostrzeżenie. W przypadku zastosowania filtru uwzględniającego operacja tworzenia kopii zapasowej się nie powiedzie.

Filtr z pełną ścieżką obejmuje literę dysku (w systemie Windows) lub katalog główny (w systemie Linux lub macOS). Na przykład pełna ścieżka pliku może wyglądać następująco: **C:\Temp\Plik.tmp**. Filtr obejmujący literę dysku lub katalog główny, na przykład **C:\Temp\Plik.tmp** lub **C:\Temp***, spowoduje wygenerowanie ostrzeżenia lub niepowodzenie operacji.

Filtr, który nie obejmuje litery dysku lub katalogu głównego (na przykład **Temp*** lub **Temp\Plik.tmp**) lub filtr zaczynający się gwiazdką (na przykład ***C:**) nie spowoduje wygenerowania ostrzeżenia ani niepowodzenia operacji. Jeśli jednak system operacyjny komputera uwzględnianego w kopii zapasowej nie zostanie poprawnie wykryty, te filtry plików również nie będą działać.

- **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 użyć jednego lub kilku 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**

[Tylko w przypadku kopii zapasowych w formacie **Wersja 12**] Dwie gwiazdki (**) zastępują zero lub więcej znaków w nazwie pliku i ścieżce, w tym znak ukośnika. Na przykład kryterium ****/Dokumenty/**.txt** oznacza wszystkie pliki TXT we wszystkich podfolderach wszystkich folderów **Dokumenty**.

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**).

Uwaga
Atrybuty plików i folderów można sprawdzić w ich właściwościach lub przy użyciu polecenia attrib. Więcej informacji można znaleźć w Centrum pomocy i obsługi technicznej w systemie Windows.

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.

Ustawienie wstępne:

- Jeśli do uwzględnienia w kopii zapasowej wybrano tylko komputery z systemem Linux: **Nie twórz migawki.**
- W przeciwnym razie: **Utwórz migawkę, jeśli to możliwe.**

Można 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.

Dane do analizy śledczej

Złośliwe działania na komputerze mogą być wykonywane przez wirusy, złośliwe oprogramowanie i oprogramowanie wymuszające okup. Innym przypadkiem, który może wymagać zbadania, jest kradzież lub zmiana danych na komputerze za pomocą różnych programów. Takie działania mogą wymagać zbadania, ale jest to możliwe tylko wtedy, gdy na komputerze są przechowywane dowody cyfrowe na potrzeby prac dochodzeniowych. Niestety, dowody (pliki, ślady itd.) mogą zostać usunięte lub komputer może przestać być dostępny.

Opcja tworzenia kopii zapasowej o nazwie **Dane do analizy śledczej** umożliwia zbieranie dowodów cyfrowych, które można wykorzystać w dochodzeniach śledczych. Jako dowód cyfrowy mogą posłużyć następujące elementy: migawka nieużywanego miejsca na dysku, zrzuty pamięci oraz migawka uruchomionych procesów. Funkcja **Dane do analizy śledczej** jest dostępna tylko w przypadku tworzenia kopii zapasowej całego komputera.

Obecnie opcja **Dane do analizy śledczej** jest dostępna tylko w przypadku komputerów z systemem Windows w następujących wersjach:

- Windows 8.1, Windows 10
- Windows Server 2012 R2 — Windows Server 2019

Uwaga
• Po zastosowaniu do komputera planu ochrony przy użyciu modułu Kopia zapasowa nie będzie można zmodyfikować ustawień danych do analizy śledczej. Aby skorzystać z innych ustawień w odniesieniu do danych do analizy śledczej, należy utworzyć nowy plan ochrony.
• Kopie zapasowe z danymi do analizy śledczej nie są obsługiwane w przypadku komputerów mających z siecią połączenie VPN i niemających bezpośredniego dostępu do Internetu.

Obsługiwane lokalizacje kopii zapasowych na potrzeby analizy śledczej:

- Chmura
- Folder lokalny

  Uwaga
  1. Folder lokalny jest obsługiwany tylko na zewnętrznym dysku twardym podłączonym przez port USB.
  2. Lokalne dyski dynamiczne nie są obsługiwane jako lokalizacja kopii zapasowych na potrzeby analizy śledczej.

- Folder sieciowy

Kopie zapasowe na potrzeby analizy śledczej są automatycznie notaryzowane. Tworzenie kopii zapasowych na potrzeby analizy śledczej pozwoli prowadzącym dochodzenie na analizę tych obszarów dysku, które zwykle nie są uwzględniane w jego zwykłej kopii zapasowej.

Proces tworzenia kopii zapasowej na potrzeby analizy śledczej

Podczas tworzenia kopii zapasowej na potrzeby analizy śledczej system wykonuje następujące czynności:

1. Zapisuje surowy zrzut pamięci i listę uruchomionych procesów.
2. Automatycznie uruchamia ponownie komputer przy użyciu nośnika startowego.
3. Tworzy kopię zapasową, która zawiera zarówno zajmowane, jak i niealokowane miejsce.
4. Notaryzuje dyski uwzględniane w kopii zapasowej.
5. Uruchamia się ponownie w trybie systemu operacyjnego na żywo i kontynuuje wykonywanie planu (np. replikację, przechowywanie, sprawdzenie poprawności i inne).

Aby skonfigurować zbieranie danych do analizy śledczej

1. W konsoli internetowej Cyber Protect przejdź do sekcji **Urządzenia** > **Wszystkie urządzenia**. Plan ochrony można też utworzyć na karcie **Plany**.
2. Wybierz urządzenie i kliknij **Chroń**.
3. W planie ochrony w ustawieniach modułu Kopia zapasowa włącz moduł **Kopia zapasowa**.
4. W polu **Elementy uwzględniane w kopii zapasowej** wybierz **Cały komputer**.
5. W sekcji **Opcje tworzenia kopii zapasowych** kliknij **Zmień**.
6. Znajdź opcję **Dane do analizy śledczej**.
7. Włącz **Zbierz dane do analizy śledczej**. System automatycznie pobierze zrzut pamięci i utworzy migawkę uruchomionych procesów.

   Uwaga
   Pełny zrzut pamięci może zawierać poufne dane, na przykład hasła.

8. Podaj lokalizację.
9. Kliknij **Uruchom teraz**, aby niezwłocznie utworzyć kopię zapasową z danymi do analizy śledczej, lub poczekaj na utworzenie kopii zapasowej zgodnie z harmonogramem.
10. Przejdź do sekcji **Panel** > **Działania** i sprawdź, czy kopia zapasowa z danymi do analizy śledczej została pomyślnie utworzona.

W wyniku tych działań kopie zapasowe będą zawierały dane do analizy śledczej, które będzie można pobrać i przeanalizować. Kopie zapasowe z danymi do analizy śledczej są oznaczone i można je wyfiltrować spośród innych kopii zapasowych w sekcji **Magazyn kopii zapasowych** > **Lokalizacje** za pomocą opcji **Tylko z danymi do analizy śledczej**.

Jak pobrać dane do analizy śledczej z kopii zapasowej?

1. W konsoli internetowej Cyber Protect przejdź do sekcji **Magazyn kopii zapasowych** i wybierz lokalizację z kopiami zapasowymi zawierającymi dane do analizy śledczej.

2. Zaznacz odpowiednią kopię zapasową z danymi do analizy śledczej i kliknij **Pokaż kopie zapasowe**.
3. Kliknij **Odzyskaj** w wierszu właściwej kopii zapasowej.
   - Aby odzyskać tylko dane do analizy śledczej, kliknij **Dane do analizy śledczej**.
     System wyświetli folder z danymi do analizy śledczej. Wybierz plik zrzutu pamięci lub dowolny inny plik przeznaczony do analizy śledczej i kliknij **Pobierz**.
   - Aby odzyskać całą kopię zapasową z danymi do analizy śledczej, kliknij **Cały komputer**.
     System odzyska kopię zapasową bez trybu startowego. Dzięki temu będzie można sprawdzić, czy dysk nie został zmieniony.

Dostępny zrzut pamięci można poddać dogłębniejszym analizom za pomocą kilku programów do analizy śledczej innych firm, na przykład programu Volatility Framework: https://www.volatilityfoundation.org/.

Notaryzacje kopii zapasowych z danymi do analizy śledczej

Aby umożliwić sprawdzenie, czy kopia zapasowa z danymi do analizy śledczej jest dokładnie tym samym obrazem, który został utworzony, tj. że nie został on naruszony, moduł Kopia zapasowa dokonuje notaryzacji kopii zapasowych z danymi do analizy śledczej.

Sposób działania

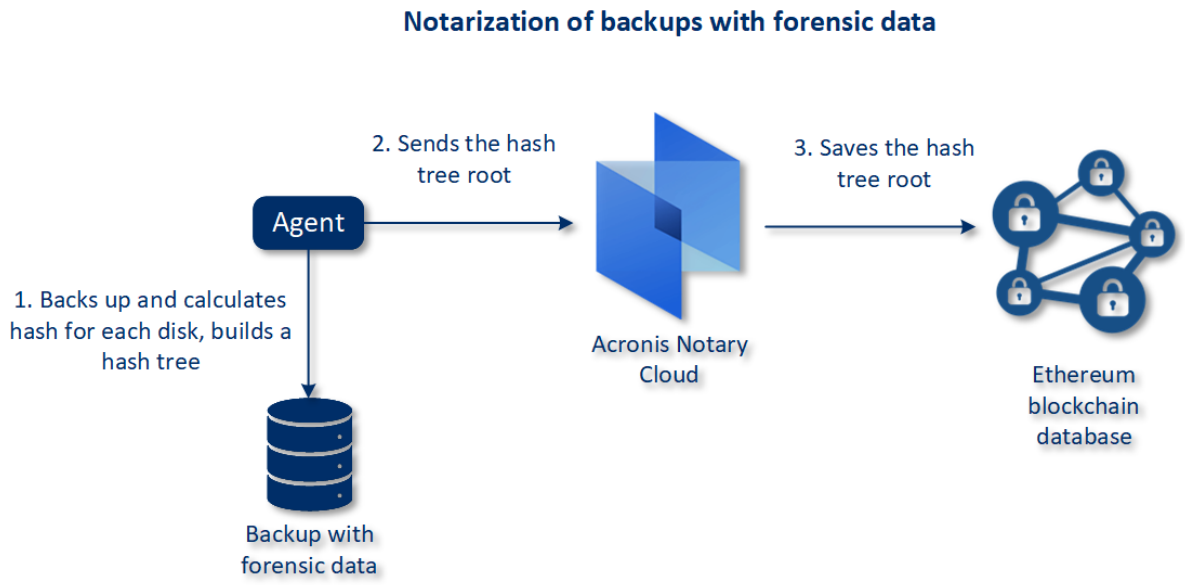
Notaryzacja pozwala udowodnić, że dysk z danymi do analizy śledczej jest autentyczny i niezmieniony od chwili uwzględnienia w kopii zapasowej.

Podczas tworzenia kopii zapasowej agent oblicza kody skrótów uwzględnianych w kopii dysków, buduje drzewo skrótów, zapisuje drzewo w kopii zapasowej, a następnie wysyła główne drzewo skrótów do usługi notaryzacji. Usługa notaryzacji zapisuje główne drzewo skrótów w bazie danych łańcucha bloków Ethereum, aby zapewnić, że ta wartość nie zostanie zmieniona.

Weryfikując autentyczność dysku z danymi do analizy śledczej, agent oblicza jego skrót, a następnie porównuje go ze skrótem przechowywanym w drzewie skrótów w kopii zapasowej. W przypadku niezgodności skrótów uznaje się, że dysk nie jest autentyczny. W przeciwnym razie autentyczność dysku jest gwarantowana przez drzewo skrótów.

Aby zweryfikować, czy samo drzewo skrótów nie zostało naruszone, agent wysyła główne drzewo skrótów do usługi notaryzacji. Usługa notaryzacji porównuje je z drzewem przechowywanym w bazie danych łańcucha bloków. Jeśli skróty są zgodne, wybrany dysk na pewno jest autentyczny. W przeciwnym razie program wyświetla komunikat, że dysk nie jest autentyczny.

Poniższy schemat obrazuje w skrócie proces notaryzacji kopii zapasowych z danymi do analizy śledczej.



Aby ręcznie zweryfikować notaryzowaną kopię zapasową dysku, można uzyskać dla niej certyfikat i postąpić zgodnie z wyświetlaną procedurą weryfikacji przy użyciu certyfikatu, korzystając z narzędzia tibxread.

Uzyskiwanie certyfikatu na potrzeby kopii zapasowych z danymi do analizy śledczej

Aby uzyskać z konsoli certyfikat na potrzeby kopii zapasowej z danymi do analizy śledczej:

1. Przejdź do sekcji **Magazyn kopii zapasowych** i zaznacz kopię zapasową z danymi do analizy śledczej.
2. Odzyskaj cały komputer.
3. System otworzy się w widoku **Mapowanie dysków**.
4. Kliknij ikonę **Uzyskaj certyfikat** w wierszu dysku.
5. System wygeneruje certyfikat i otworzy go w nowym oknie przeglądarki. Pod certyfikatem będzie dostępna instrukcja ręcznej weryfikacji notaryzowanej kopii zapasowej dysku.

Narzędzie „tibxread” do pobierania danych z kopii zapasowej

Cyber Protect udostępnia narzędzie `tibxread`, które umożliwia ręczne sprawdzenie integralności dysku z kopii zapasowej. Narzędzie to pozwala na pobranie danych z kopii zapasowej i obliczenie skrótu wybranego dysku. Jest ono instalowane automatycznie wraz z następującymi komponentami: agent dla systemu Windows, agent dla systemu Linux i agent dla system Mac. Znajduje się w folderze: `C:\Program Files\Acronis\BackupAndRecovery`.

Obsługiwane lokalizacje:

- Dysk lokalny
- Folder sieciowy (CIFS/SMB), który jest dostępny bez wymaganych poświadczeń.

W przypadku folderu sieciowego chronionego hasłem można za pomocą narzędzi systemu operacyjnego zamontować folder sieciowy do folderu lokalnego, a następnie użyć tego folderu lokalnego jako źródła dla narzędzia.

- Chmura

  Należy podać adres URL, port i certyfikat. Adres URL i port można uzyskać z klucza rejestru systemu Windows lub plików konfiguracyjnych na komputerach z systemem Linux/Mac.

  W przypadku systemu Windows:

  ```
  HKEY_LOCAL_
  MACHINE\SOFTWARE\Acronis\BackupAndRecovery\Settings\OnlineBackup\FesAddressCache\Defa
  ult\<tenant_login>\FesUri
  ```

  W przypadku systemu Linux:

  ```
  /etc/Acronis/BackupAndRecovery.config
  ```

  W przypadku systemu macOS:

  ```
  /Library/Application Support/Acronis/Registry/BackupAndRecovery.config
  ```

  Certyfikat można znaleźć w następujących lokalizacjach:

  W przypadku systemu Windows:

  ```
  %allusersprofile%\Acronis\BackupAndRecovery\OnlineBackup\Default
  ```

  W przypadku systemu Linux:

  ```
  /var/lib/Acronis/BackupAndRecovery/OnlineBackup/Default
  ```

  W przypadku systemu macOS:

  ```
  /Library/Application Support/Acronis/BackupAndRecovery/OnlineBackup/Default
  ```

Narzędzie obsługuje następujące polecenia:

- list backups
- list content
- get content
- calculate hash

list backups

Umożliwia wyświetlenie listy punktów odzyskiwania dostępnych w kopii zapasowej.

SKŁADNIA:

```
tibxread list backups --loc=URI --arc=BACKUP_NAME --raw
```

Opcje

```
--loc=URI
--arc=BACKUP_NAME
--raw
--utc
--log=PATH
```

```
Output template:
```

```
GUID   Date   Date timestamp
----   ------ --------------
<guid> <date> <timestamp>
```

<guid> — identyfikator GUID kopii zapasowej.

<date> — data utworzenia kopii zapasowej. Ma ona następujący format: DD.MM.RRRR GG24:MM:SS. Domyślnie w lokalnej strefie czasowej (można ją zmienić za pomocą opcji --utc).

Przykład danych wyjściowych:

```
GUID   Date   Date timestamp
----   ------ --------------
516FCE73-5E5A-49EF-B673-A9EACB4093B8 18.12.2019 16:01:05 1576684865
516FCE73-5E5A-49EF-B673-A9EACB4093B9 18.12.2019 16:02:05 1576684925
```

list content

Umożliwia wyświetlenie listy zawartości punktu odzyskiwania.

SKŁADNIA:

```
tibxread list content --loc=URI --arc=BACKUP_NAME --password --backup=RECOVERY_POINT_ID
--raw --log=PATH
```

Opcje

```
--loc=URI
--arc=BACKUP_NAME
--password
--backup=RECOVERY_POINT_ID
--raw
--log=PATH
```

Wzór danych wyjściowych:

```
Disk     Size   Notarization status
-------- ------ --------------------
<number> <size> <notarization_status>
```

<number> — identyfikator dysku.

<size> — rozmiar w bajtach.

<notarization_status> — możliwe są następujące statusy: Bez notaryzacji, Notaryzowano, Następna kopia zapasowa.

Przykład danych wyjściowych:

```
Disk     Size   Notary status
-------- ------ --------------
1        123123465798 Notarized
2        123123465798 Notarized
```

get content

Umożliwia zapisanie zawartości wskazanego dysku w punkcie odzyskiwania na standardowym wyjściu danych (stdout).

SKŁADNIA:

```
tibxread get content --loc=URI --arc=BACKUP_NAME --password --backup=RECOVERY_POINT_ID -
-disk=DISK_NUMBER --raw --log=PATH --progress
```

Opcje

```
--loc=URI
--arc=BACKUP_NAME
--password
--backup=RECOVERY_POINT_ID
--disk=DISK_NUMBER
--raw
--log=PATH
--progress
```

calculate hash

Umożliwia obliczenie skrótu wskazanego dysku w punkcie odzyskiwania za pomocą algorytmu SHA-256 i zapisanie go na wyjściu stdout.

SKŁADNIA:

```
tibxread calculate hash --loc=URI --arc=BACKUP_NAME --password --backup=RECOVERY_POINT_
ID --disk=DISK_NUMBER --raw --log=PATH --progress
```

Opcje

```
--loc=URI
--arc=BACKUP_NAME
--password
--backup=RECOVERY_POINT_ID
```

```
--disk=DISK_NUMBER
--raw
--log=PATH
```

Opis opcji

Opcja	Opis
--arc=NAZWA_KOPII_ZAPASOWEJ	Nazwę pliku kopii zapasowej można znaleźć we właściwościach kopii zapasowej w konsoli internetowej. Nazwę pliku kopii zapasowej należy podać wraz z rozszerzeniem .tibx.
--backup=IDENTYFIKATOR_PUNKTU_ODZYSKIWANIA	Identyfikator punktu odzyskiwania.
--disk=NUMER_DYSKU	Numer dysku (ten sam, który został zapisany w danych wyjściowych polecenia „get content”).

--loc=IDENTYFIKATOR_URI	Identyfikator URI lokalizacji kopii zapasowej. Możliwe formaty opcji „--loc”:
	• Nazwa ścieżki lokalnej (Windows)
	`c:/upload/backups`
	• Nazwa ścieżki lokalnej (Linux)
	`/var/tmp`
	• SMB/CIFS
	`\\server\folder`
	• Chmura
	`--loc=<IP_address>:443 --cert=<path_to_certificate> [--storage_path=/1]`
	<adres_IP> — można go znaleźć w kluczu rejestru w systemie Windows: HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\BackupAndRecovery\Settings\OnlineBackup\FesAddressCache\Default\<nazwa_logowania_dzierżawcy>\FesUri
	<ścieżka_do_certyfikatu> — ścieżka do pliku certyfikatu używanego w celu uzyskania dostępu do platformy Cyber Cloud. Na przykład w systemie Windows certyfikat można znaleźć w folderze `C:\ProgramData\Acronis\BackupAndRecovery\OnlineBackup\Default\<nazwa_użytkownika>.crt`, gdzie <nazwa_użytkownika> jest nazwą konta używanego w celu uzyskania dostępu do platformy Cyber Cloud.

--log=ŚCIEŻKA	Aktywuje zapisywanie dzienników w określonej ŚCIEŻCE (tylko ścieżka lokalna, format jest taki sam jak w przypadku parametru `--loc=URI`). Stosowany jest poziom dziennika DEBUG.
--password=HASŁO	Hasło szyfrowania kopii zapasowej. Jeśli kopia zapasowa nie jest zaszyfrowana, pozostaw tę wartość pustą.

--raw	Umożliwia ukrycie nagłówków (dwóch pierwszych wierszy) w danych wyjściowych polecenia. Jest używany w sytuacji, gdy powinny być analizowane dane wyjściowe polecenia.
	Przykład danych wyjściowych bez parametru „`--raw`”:
	`GUID Date Date timestamp`
	`---- ------ --------------`
	`516FCE73-5E5A-49EF-B673-A9EACB4093B8 18.12.2019 16:01:05 1576684865`
	`516FCE73-5E5A-49EF-B673-A9EACB4093B9 18.12.2019 16:02:05 1576684925`
	Dane wyjściowe z parametrem „`--raw`”:
	`516FCE73-5E5A-49EF-B673-A9EACB4093B8 18.12.2019 16:01:05 1576684865`
	`516FCE73-5E5A-49EF-B673-A9EACB4093B9 18.12.2019 16:02:05 1576684925`

--utc	Umożliwia wyświetlenie dat w standardzie UTC.

--progress	Umożliwia wyświetlenie postępu operacji.
	Na przykład:
	`1%`
	`2%`
	`3%`
	`4%`
	`...`
	`100%`

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: **Włączono**.

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.

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.

Punkty zamontowania

Ta opcja jest dostępna tylko w systemie Windows na potrzeby tworzenia kopii zapasowych na poziomie plików uwzględniającej źródło danych obejmujące zamontowane woluminy lub udostępnione woluminy klastra.

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).

- W przypadku wybrania takiego folderu (folderu nadrzędnego) do uwzględnienia w kopii zapasowej i włączenia opcji **Punkty zamontowania** w kopii zapasowej zostaną uwzględnione wszystkie pliki znajdujące się w zamontowanym woluminie. Jeśli opcja **Punkty zamontowania** będzie wyłączona, punkt zamontowania w kopii zapasowej będzie pusty.
  Odzyskanie zawartości punktu zamontowania podczas odzyskiwania folderu nadrzędnego zależy od włączenia lub wyłączenia opcji **Punkty zamontowania** w ramach operacji odzyskiwania.
- 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 **Punkty zamontowania** w ramach operacji odzyskiwania.

Ustawienie wstępne: **Wyłączono**.

Uwaga
Można tworzyć kopie zapasowe maszyn wirtualnych Hyper-V znajdujących się na udostępnionym woluminie klastra, uwzględniając w niej wymagane pliki lub cały wolumin w ramach tworzenia kopii zapasowej na poziomie plików. Należy tylko pamiętać o wyłączeniu maszyn wirtualnych, aby ich kopia zapasowa była spójna.

Przykład

Załóżmy, że folder **C:\Dane1** jest punktem zamontowania woluminu. Wolumin zawiera foldery **Folder1** i **Folder2**. Tworzysz plan ochrony na potrzeby kopii zapasowej danych na poziomie plików.

Jeśli zaznaczysz pole wyboru woluminu C i włączysz opcję **Punkty zamontowania**, folder **C:\Dane1** w kopii zapasowej będzie zawierać foldery **Folder1** i **Folder2**. W przypadku odzyskiwania danych z kopii zapasowej należy pamiętać o poprawnym zastosowaniu opcji **Punkty zamontowania** w ramach operacji odzyskiwania.

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**, folder **Folder1** lub **Folder2**, zaznaczone foldery zostaną uwzględnione w kopii zapasowej jako zwykłe foldery bez względu na stan opcji **Punkty zamontowania**.

Migawka wielowoluminowa

Ta opcja jest dostępna w przypadku kopii zapasowych komputerów fizycznych z systemem Windows lub Linux.

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 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:

- Jeśli do uwzględnienia w kopii zapasowej wybrano co najmniej jeden komputer z systemem Windows: **Włączono**.
- Jeśli nie wybrano żadnych komputerów (tak jest w przypadku rozpoczęcia opracowywania planu ochrony na stronie **Plany** > **Kopia zapasowa**): **Włączono**.
- W przeciwnym razie: **Wyłączono**.

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.

Odzyskiwanie jednym kliknięciem

Funkcja Odzyskiwanie jednym kliknięciem umożliwia użytkownikowi automatyczne odzyskanie najnowszej kopii zapasowej dysku. Może to być kopia zapasowa całego komputera lub kopia zapasowa jego wybranych dysków/woluminów.

Funkcja ta jest dostępna na komputerze użytkownika po aktywowaniu jej przez administratora w połączeniu z narzędziem Startup Recovery Manager. Administrator może wykonać tę operację tylko przy użyciu interfejsu wiersza polecenia. Aby dowiedzieć się więcej o tym, jak aktywować narzędzie Startup Recovery Manager i funkcję Odzyskiwanie jednym kliknięciem, zapoznaj się z sekcją Opis wiersza polecenia.

Funkcja Odzyskiwanie jednym kliknięciem obsługuje następujące magazyny kopii zapasowych:

1. Secure Zone
2. Magazyn sieciowy
3. Chmura

Jeśli określony typ magazynu nie jest dostępny lub nie ma w nim kopii zapasowych dysków, pojawi się monit o użycie następnego typu magazynu.

Jeśli w magazynie jest dostępny więcej niż jeden zestaw kopii zapasowych (nazywany także *archiwum*), który obejmuje kopie zapasowe dysków, funkcja Odzyskiwanie jednym kliknięciem wybierze zestaw kopii zapasowych zaktualizowany jako ostatni. Nie możesz wybrać innego zestawu kopii zapasowych.

Funkcja Odzyskiwanie jednym kliknięciem obsługuje następujące operacje:

- Automatyczne odzyskiwanie z ostatniej kopii zapasowej
- Odzyskiwanie z określonej kopii zapasowej (nazywanej też *punktem odzyskiwania*) z automatycznie wybranego zestawu kopii zapasowych

Odzyskiwanie komputera przy użyciu funkcji Odzyskiwanie jednym kliknięciem

Wymagania wstępne

- Administrator włączył funkcję Odzyskiwanie jednym kliknięciem na wybranym komputerze.
- Istnieje co najmniej jedna kopia zapasowa dysku wybranego komputera.

Aby odzyskać komputer

1. Uruchom ponownie komputer, który chcesz odzyskać.
2. Podczas uruchamiania ponownie naciśnij klawisz F11, aby otworzyć narzędzie Startup Recovery Manager.
3. Wybierz odpowiednią opcję funkcji Odzyskiwanie jednym kliknięciem:
   - Aby automatycznie odzyskać ostatnią kopię zapasową, naciśnij klawisz 1.
   - Aby odzyskać inną kopię zapasową z ostatnio zaktualizowanego zestawu kopii zapasowych, naciśnij klawisz 2.
     - Aby wybrać kopię zapasową (nazywaną również *punktem odzyskiwania*), naciśnij klawisz z cyfrą odpowiadającą numerowi kopii.

Zostanie uruchomiony graficzny interfejs użytkownika, a następnie zniknie. Procedura odzyskiwania będzie kontynuowana bez niego. Po zakończeniu operacji odzyskiwania komputer zostanie uruchomiony ponownie.

Wydajność i okno na utworzenie kopii zapasowej

Ta opcja umożliwia ustawienie jednego z trzech poziomów wydajności tworzenia kopii zapasowej (wysoki, niski, zabroniony) dla każdej godziny w tygodniu. W ten sposób można definiować przedziały czasu, w których operacje tworzenia kopii zapasowych mogą być uruchamiane i wykonywane. Niski i wysoki poziom wydajności można też skonfigurować przez określenie priorytetu procesów i szybkości danych wyjściowych.

Opcja ta nie jest dostępna w przypadku operacji tworzenia kopii zapasowych wykonywanych przez agentów w chmurze, np. kopii zapasowych witryn internetowych lub kopii zapasowych serwerów znajdujących się w lokalizacji odzyskiwania w chmurze.

Opcję tę można skonfigurować osobno dla każdej lokalizacji określonej w planie ochrony. Aby ją skonfigurować dla lokalizacji replikacji, kliknij ikonę koła zębatego widoczną obok nazwy lokalizacji, a następnie kliknij **Wydajność i okno na utworzenie kopii zapasowej**.

Ta opcja działa tylko w przypadku procesów tworzenia i replikacji kopii zapasowych. Polecenia wykonywane po utworzeniu kopii zapasowej i inne operacje uwzględnione w planie ochrony (sprawdzanie poprawności, konwersja na maszynę wirtualną) będą wykonywane niezależnie od tej opcji.

Ustawienie wstępne: **Wyłączone**.

Gdy ta opcja jest wyłączona, operacje tworzenia kopii zapasowych mogą być uruchamiane w każdej chwili, z zastosowaniem następujących parametrów (bez względu na to, czy ich wartości zostały zmienione w stosunku do wartości predefiniowanych):

- Priorytet procesora: **Niski** (w systemie Windows odpowiada ustawieniu **Poniżej normalnego**).
- Szybkość danych wyjściowych: **Bez ograniczeń**.

Gdy ta opcja jest włączona, zaplanowane kopie zapasowe są dozwolone lub blokowane zgodnie z parametrami wydajności określonymi dla danej godziny. Na początku godziny, w której kopie

zapasowe są blokowane, proces tworzenia kopii zapasowej zostanie automatycznie zatrzymany i zostanie wygenerowany alert.

Nawet jeśli zaplanowane operacje tworzenia kopii zapasowych są blokowane, można je uruchomić ręcznie. Jeśli operacje tworzenia kopii zapasowych są dozwolone, zostaną użyte parametry wydajności z ostatniej godziny.

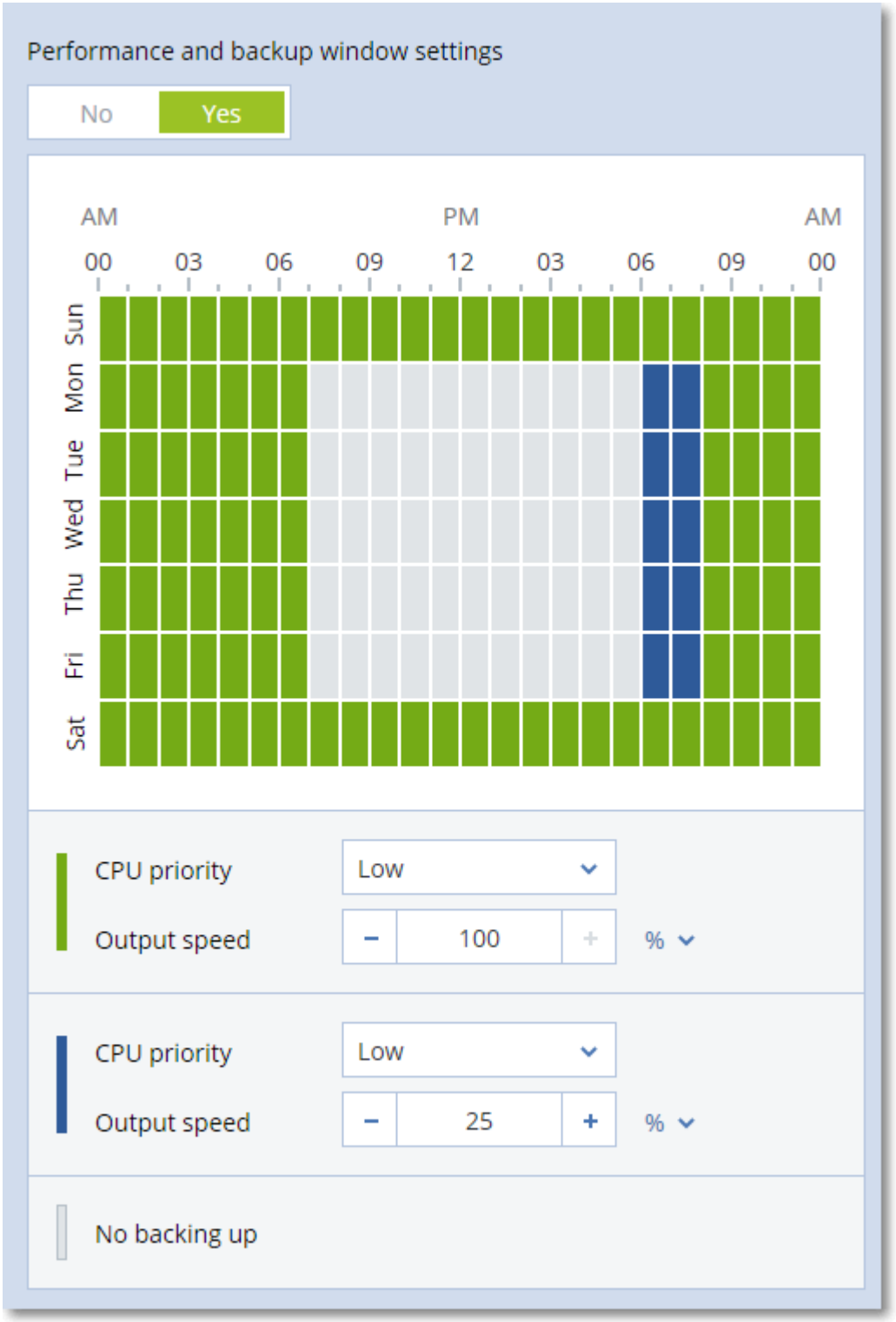
Okno na utworzenie kopii zapasowej

Każdy prostokąt odzwierciedla godzinę w dniu tygodnia. Klikaj prostokąt, aby przełączać między następującymi stanami:

- **Zielony:** operacja tworzenia kopii zapasowej jest dozwolona — z parametrami określonymi w zielonej sekcji poniżej.
- **Niebieski:** operacja tworzenia kopii zapasowej jest dozwolona — z parametrami określonymi w niebieskiej sekcji poniżej.

  Jeśli kopia zapasowa ma ustawiony format **Wersja 11**, ten stan jest niedostępny.
- **Szary:** operacja tworzenia kopii zapasowej jest blokowana.

Aby zmienić stan wielu prostokątów naraz, można kliknąć i przeciągnąć myszą.



Priorytet procesora

Ten parametr umożliwia określenie priorytetu procesu tworzenia kopii zapasowej w systemie operacyjnym.

Dostępne są następujące ustawienia:

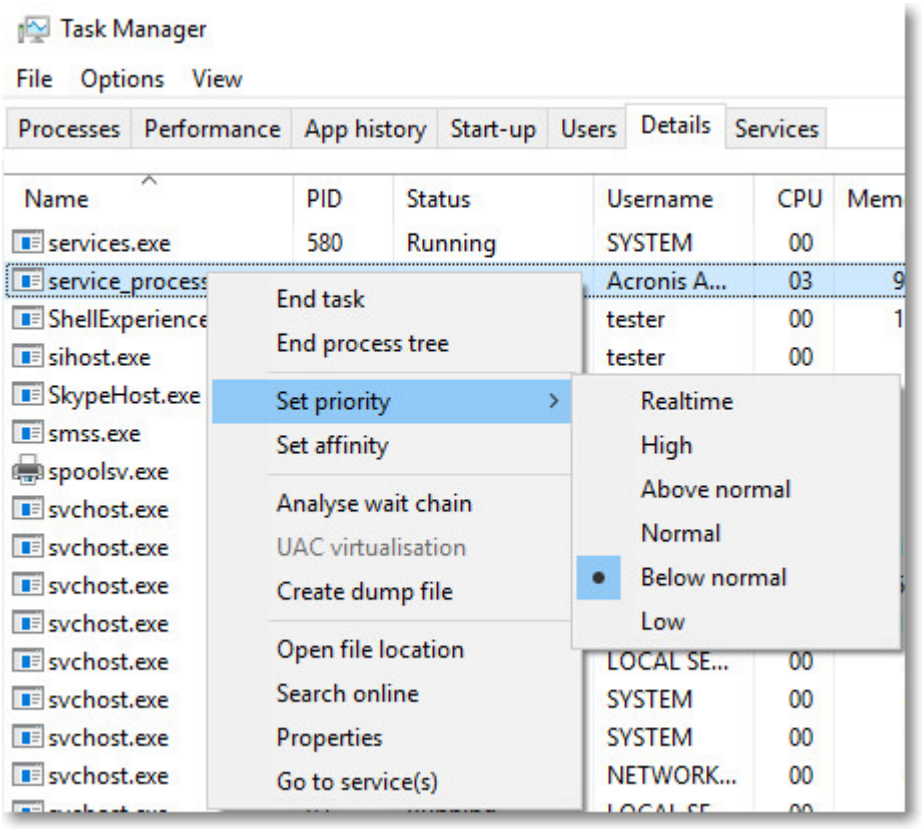
Niski — w systemie Windows odpowiada ustawieniu **Poniżej normalnego**.

Normalny — w systemie Windows odpowiada ustawieniu **Normalny**.

Wysoki — w systemie Windows odpowiada ustawieniu **Wysoki**.

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.

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

Ten parametr 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).

W przypadku włączenia tej opcji można określić maksymalną dozwoloną szybkość danych wyjściowych:

- Jako procent szacowanej szybkości zapisu na docelowym dysku twardym (gdy kopia zapasowa jest tworzona w folderze lokalnym) lub szacowanej maksymalnej szybkości połączenia sieciowego (gdy kopia zapasowa jest tworzona w udziale sieciowym lub chmurze).

  To ustawienie działa tylko wtedy, gdy agent jest uruchomiony w systemie Windows.
- W KB/s (w przypadku wszystkich lokalizacji docelowych).

Fizyczne dostarczanie danych

Ta opcja działa, jeśli lokalizacją docelową kopii zapasowych jest chmura, a format kopii zapasowej jest ustawiony jako **Wersja 12**.

Ta opcja działa w przypadku kopii zapasowych na poziomie dysku i kopii zapasowych plików tworzonych przez agenta dla systemu Windows, agenta dla systemu Linux, agenta dla systemu Mac, agenta dla VMware oraz agenta dla Hyper-V. Kopie zapasowe tworzone przy użyciu nośnika startowego nie są obsługiwane.

Ta opcja określa, czy pierwsza pełna kopia zapasowa utworzona w ramach planu ochrony zostanie przesłana do chmury na dysku twardym przy użyciu usługi Fizyczne dostarczanie danych. Kolejne przyrostowe kopie zapasowe mogą już być wykonywane przez sieć.

Ustawienie wstępne: **Wyłączono.**

Informacje o usłudze Fizyczne dostarczanie danych

Interfejs internetowy usługi Fizyczne dostarczanie danych jest dostępny tylko dla administratorów organizacji w ramach wdrożeń lokalnych oraz administratorów w ramach wdrożeń chmurowych.

Szczegółowe instrukcje korzystania z usługi Fizyczne dostarczanie danych oraz narzędzie do tworzenia zamówień można znaleźć w Podręczniku administratora usługi Fizyczne dostarczanie danych. W celu uzyskania dostępu do tego dokumentu w ramach interfejsu internetowego usługi Fizyczne dostarczanie danych kliknij ikonę ze znakiem zapytania.

Omówienie procesu fizycznego dostarczania danych

1. Utwórz nowy plan ochrony. W ramach tego planu włącz opcję tworzenia kopii zapasowych **Fizyczne dostarczanie danych**.

   Kopie zapasowe możesz utworzyć bezpośrednio na wybranym dysku albo w folderze lokalnym bądź sieciowym, a następnie skopiować je lub przenieść na ten dysk.

   Ważne
   Po utworzeniu pierwszej pełnej kopii zapasowej kolejne kopie zapasowe muszą być tworzone w ramach tego samego planu ochrony. Inny plan ochrony, nawet mający takie same parametry i dotyczący tego samego komputera, będzie wymagać innego cyklu fizycznego dostarczania danych.

2. Po utworzeniu pierwszej kopii zapasowej należy za pomocą interfejsu internetowego usługi Fizyczne dostarczanie danych pobrać narzędzie do tworzenia zamówień i utworzyć zamówienie.

Aby uzyskać dostęp do interfejsu internetowego, wykonaj jedną z następujących czynności:

- W ramach wdrożeń lokalnych: zaloguj się na koncie Acronis i kliknij **Przejdź do konsoli monitorowania** w obszarze **Fizyczne dostarczanie danych**.
- W ramach wdrożeń w chmurze: zaloguj się do portalu zarządzania, kliknij **Przegląd** > **Wykorzystanie**, a następnie kliknij **Zarządzaj usługą** w obszarze **Fizyczne dostarczanie danych**.

3. Zapakuj dyski i wyślij je do centrum danych.

Ważne
Koniecznie przestrzegaj instrukcji dotyczących pakowania zawartych w Podręczniku administratora usługi Fizyczne dostarczanie danych.

4. Status zamówienia możesz monitorować w interfejsie internetowym usługi Fizyczne dostarczanie danych. Pamiętaj, że dopóki pierwsza kopia zapasowa nie zostanie przesłana do chmury, kolejne operacje tworzenia kopii zapasowych będą się kończyć niepowodzeniem.

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

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

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

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 wybierz plik wsadowy. Program nie obsługuje poleceń interaktywnych, czyli wymagających wpisania tekstu przez użytkownika (na przykład „pause").
3. W polu **Katalog roboczy** wpisz ścieżkę do katalogu, w którym ma zostać wykonane polecenie lub plik wsadowy.
4. W polu **Argumenty** w razie potrzeby podaj argumenty wykonania 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.

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 wybierz plik wsadowy.
3. W polu **Katalog roboczy** wpisz ścieżkę do katalogu, w którym ma zostać 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 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 na karcie **Działania**.
6. Kliknij **Gotowe**.

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.

<table>
<tr><td></td><td colspan="4"><---------- Kopia zapasowa ---------- ---></td><td></td></tr>
<tr><td>Polecenie poprzedzające utworzenie kopii zapasowej</td><td>Polecenie poprzedzające rejestrowanie danych</td><td>Rejestrowanie danych</td><td>Polecenie następujące po zarejestrowaniu danych</td><td></td><td>Polecenie następujące po utworzeniu kopii zapasowej</td></tr>
</table>

Jeśli opcja 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 -> Rejestrowanie 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.

Polecenie poprzedzające rejestrowanie danych

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

1. Włącz przełącznik **Wykonaj polecenie przed zarejestrowaniem danych**.
2. W polu **Polecenie** wpisz polecenie lub wybierz plik wsadowy. Program nie obsługuje poleceń interaktywnych, czyli wymagających wpisania tekstu przez użytkownika (na przykład „pause").
3. W polu **Katalog roboczy** wpisz ścieżkę do katalogu, w którym ma zostać wykonane polecenie lub plik wsadowy.
4. W polu **Argumenty** w razie potrzeby podaj argumenty wykonania 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	Zarejestruj dane po wykonaniu polecenia, niezależnie od tego, czy zakończyło się powodzeniem, czy	N.d.	Zarejestruj dane równolegle z wykonywaniem polecenia i niezależnie od wyniku jego wykonania.

	wykonanie polecenia się nie powiedzie, zakończ tworzenie kopii zapasowej niepowodzeniem.	niepowodzeniem.		

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

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 wybierz plik wsadowy. Program nie obsługuje poleceń interaktywnych, czyli wymagających wpisania tekstu przez użytkownika (na przykład „pause").
3. W polu **Katalog roboczy** wpisz ścieżkę do katalogu, w którym ma zostać wykonane polecenie lub plik wsadowy.
4. W polu **Argumenty** w razie potrzeby podaj argumenty wykonania 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 Kontynuuj tworzenie kopii zapasowej	Kontynuuj tworzenie kopii zapasowej po wykonaniu polecenia, niezależnie od tego,	N.d.	Kontynuuj tworzenie kopii zapasowej równolegle z wykonywaniem polecenia i

	dopiero po pomyślnym wykonaniu polecenia.	czy zakończyło się powodzeniem, czy niepowodzeniem.		niezależnie od wyniku jego wykonania.

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

Migawki urządzenia SAN

Ta opcja jest dostępna w przypadku kopii zapasowych maszyn wirtualnych VMware ESXi.

Ustawienie wstępne: **Wyłączone**.

Ta opcja określa, czy podczas tworzenia kopii zapasowej mają być używane migawki sieci SAN.

W przypadku wyłączenia tej opcji zawartość dysku wirtualnego zostanie odczytana z migawki VMware. Migawka zostanie zachowana przez cały czas tworzenia kopii zapasowej.

W przypadku włączenia tej opcji zawartość dysku wirtualnego zostanie odczytana z migawki sieci SAN. Migawka VMware zostanie utworzona i zachowana na krótki czas, aby można było uzyskać spójny stan dysków wirtualnych. Jeśli odczyt z migawki sieci SAN nie będzie możliwy, tworzenie kopii zapasowej nie powiedzie się.

Przed włączeniem tej opcji sprawdź i spełnij wymagania podane w sekcji „Korzystanie z migawek urządzeń SAN”.

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.**

Można 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 ochrony na tych komputerach. Pozostaje ona niezmienna do chwili ewentualnej edycji planu ochrony 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 ochrony jest stosowany do wielu maszyn wirtualnych. Określa ona liczbę maszyn wirtualnych, których kopie zapasowe agent może utworzyć jednocześnie podczas wykonywania danego planu ochrony.

  Jeśli zgodnie z planem ochrony 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 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. Jeśli jednak agent wykonuje wiele planów ochrony, które nakładają się na siebie w czasie, liczby określone w ich opcjach są sumowane. Istnieje możliwość ograniczenia łącznej liczby maszyn wirtualnych, których kopie zapasowe może tworzyć agent w tym samym czasie — bez względu na liczbę wykonywanych przez niego planów ochrony.

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

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: **Wyłączono**.

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 miała taki sam rozmiar jak uwzględniony w niej dysk (jeśli opcja „Stopień kompresji” ma wartość **Brak**). W przypadku tworzenia kopii zapasowej dysków z nierozpoznanym lub nieobsługiwanym systemem plików oprogramowanie automatycznie przełącza się na tryb „sektor po sektorze”.

Uwaga
Nie będzie można odzyskać danych aplikacji z kopii zapasowych utworzonych w trybie sektor po sektorze.

Dzielenie

Ta opcja działa w przypadku schematów tworzenia kopii zapasowych **Zawsze pełna**, **Tygodniowe pełne, dzienne przyrostowe**, **Miesięczne pełne, tygodniowe różnicowe, dzienne przyrostowe (GFS)** i **Niestandardowe**.

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.

Zarządzanie taśmami

Opcje te mają zastosowanie, gdy miejscem docelowym kopii zapasowej jest urządzenie taśmowe.

Włącz odzyskiwanie plików z kopii zapasowych dysków przechowywanych na taśmach

Ustawienie wstępne: **Wyłączono**.

Jeśli to pole wyboru jest zaznaczone, podczas każdej operacji tworzenia kopii zapasowej program tworzy pliki pomocnicze na dysku twardym komputera, do którego jest podłączone urządzenie taśmowe. Odzyskiwanie plików z kopii zapasowych dysków będzie możliwe pod warunkiem, że te pliki pomocnicze pozostaną nienaruszone. Pliki te zostaną usunięte automatycznie po skasowaniu, usunięciu lub nadpisaniu taśmy zawierającej odpowiednie kopie zapasowe.

Poniżej przedstawiono lokalizacje tych plików pomocniczych:

- W systemach Windows XP i Server 2003: **%ALLUSERSPROFILE%\Application Data\Acronis\BackupAndRecovery\TapeLocation**.
- W systemie Windows 7 i nowszych wersjach systemu Windows: **%PROGRAMDATA%\Acronis\BackupAndRecovery\TapeLocation**.
- W systemie Linux: **/var/lib/Acronis/BackupAndRecovery/TapeLocation**.

Miejsce zajmowane przez te pliki pomocnicze jest zależne od liczby plików w odpowiedniej kopii zapasowej. W przypadku kopii zapasowej dysku zawierającego około 20 000 plików (kopia zapasowa dysku typowej stacji roboczej) pliki pomocnicze zajmują około 150 MB. Pełna kopia zapasowa serwera zawierającego 250 000 plików może spowodować utworzenie około 700 MB plików pomocniczych. Jeśli wiesz na pewno, że nie będzie konieczne odzyskiwanie pojedynczych plików, możesz to pole wyboru pozostawić wyczyszczone, aby oszczędzić miejsce na dysku.

Jeśli pliki pomocnicze nie zostały utworzone podczas tworzenia kopii zapasowej lub zostały usunięte, w dalszym ciągu można je utworzyć poprzez ponowne przeskanowanie taśm, na których znajduje się kopia zapasowa.

Wsuń taśmę z powrotem do gniazda po każdym pomyślnym utworzeniu kopii zapasowej komputera

Ustawienie wstępne: **Włączono**.

W przypadku wyłączenia tej opcji taśma pozostanie w napędzie po zakończeniu dotyczącej jej operacji. W przeciwnym razie oprogramowanie przeniesie taśmę z powrotem do gniazda, w którym znajdowała się przed operacją. Jeśli zgodnie z planem ochrony po utworzeniu kopii zapasowej są wykonywane inne operacje (np. sprawdzanie poprawności kopii zapasowej lub replikacja do innej lokalizacji), to po zakończeniu tych operacji taśma zostanie przeniesiona z powrotem do gniazda.

Jeśli są włączone ta opcja i opcja **Wysuń taśmę po każdym pomyślnym utworzeniu kopii zapasowej komputera**, taśma jest wysuwana.

Wysuń taśmy po każdym pomyślnym utworzeniu kopii zapasowej komputera

Ustawienie wstępne: **Wyłączono**.

Jeśli to pole wyboru jest zaznaczone, program wysunie taśmy po pomyślnym utworzeniu kopii zapasowej każdego komputera. Jeśli zgodnie z planem ochrony po utworzeniu kopii zapasowej są wykonywane inne operacje (np. sprawdzanie poprawności kopii zapasowej lub replikacja do innej lokalizacji), taśmy zostaną wysunięte po zakończeniu tych operacji.

Zastąp taśmę w autonomicznym napędzie taśmowym podczas tworzenia pełnej kopii zapasowej

Ustawienie wstępne: **Wyłączono**.

Opcja ta ma zastosowanie do autonomicznych napędów taśmowych. Gdy jest ona włączona, zawartość taśmy włożonej do napędu będzie zastąpiona za każdym utworzeniem pełnej kopii zapasowej.

Użyj następujących urządzeń taśmowych i napędów

Ta opcja umożliwia określenie urządzeń taśmowych i napędów taśmowych, które mają być używane w przypadku danego planu ochrony.

Pula taśm obejmuje taśmy ze wszystkich urządzeń taśmowych podłączonych do komputera, bez względu na to, czy jest to węzeł magazynowania, czy komputer, na którym jest zainstalowany agent ochrony, czy jedno i drugie. W przypadku wybrania puli taśm jako lokalizacji kopii zapasowej pośrednio zostaje wybrany komputer, do którego są podłączone dane urządzenia taśmowe. Domyślnie kopie zapasowe mogą być zapisywane na taśmach przez dowolny napęd taśmowy

w dowolnym urządzeniu taśmowym podłączonym do tego komputera. Jeśli brakuje niektórych urządzeń lub napędów bądź z jakichś powodów one nie działają, w planie ochrony zostaną użyte dostępne urządzenia i napędy.

Kliknij **Tylko wybrane urządzenia i napędy**, a następnie wybierz urządzenia i napędy taśmowe z listy. Wybierając całe urządzenie, wybierasz wszystkie jego napędy. W związku z tym każdy z tych napędów może zostać użyty w planie ochrony. Jeśli brakuje wybranego urządzenia lub napędu bądź z jakichś powodów one nie działają, a nie wybrano żadnych innych urządzeń, operacja tworzenia kopii zapasowa się nie powiedzie.

Za pomocą tej opcji można sterować operacjami tworzenia kopii zapasowych wykonywanymi przez wielu agentów przy użyciu dużej biblioteki taśm z wieloma napędami. Na przykład operacja tworzenia kopii zapasowej dużego serwera plików lub udziału plikowego może się nie rozpocząć, jeśli wielu agentów tworzy kopie zapasowe swoich komputerów w ramach tego samego okna na utworzenie kopii zapasowych, ponieważ agenci zajmują wszystkie napędy. Jeśli pozwolisz agentom na korzystanie np. z napędów 2 i 3, napęd 1 zostanie zarezerwowany dla agenta tworzącego kopię zapasową udziału.

Obsługa wielu strumieni

Ustawienie wstępne: **Wyłączono**.

Obsługa wielu strumieni umożliwia podzielenie danych od jednego agenta na wiele strumienie, a następnie zapisanie tych strumieni na różnych taśmach w tym samym czasie. Spowoduje to szybsze tworzenie kopii zapasowych i jest szczególnie przydatne w sytuacji, gdy agent ma do dyspozycji większą przepustowość niż napęd taśmowy.

Pole wyboru **Obsługa wielu strumieni** jest dostępne tylko wtedy, gdy w obszarze **Tylko wybrane urządzenia i napędy** zostanie wybrany więcej niż jeden napęd taśmowy. Liczba wybranych napędów jest równa liczbie równoczesnych strumieni od agenta. Jeśli którykolwiek z wybranych napędów nie jest dostępny po uruchomieniu operacji tworzenia kopii zapasowej, operacja się nie powiedzie.

Do odzyskania kopii zapasowej utworzonej przy użyciu wielu strumieni lub taśmy multipleksowej potrzeba co najmniej tylu napędów, ilu użyto do utworzenia tej kopii.

Ustawień wielu strumieniu w istniejącym już planie ochrony nie można zmienić. Aby użyć innych ustawień lub zmienić wybrane napędy taśmowe, utwórz nowy plan ochrony.

Obsługa wielu strumieni jest dostępna zarówno w przypadku lokalnie podłączonych napędów taśmowych, jak i napędów taśmowych podłączonych do węzła magazynowania.

Multipleksowanie

Ustawienie wstępne: **Wyłączono**.

Multipleksowanie umożliwia zapisywanie strumieni danych od wielu agentów na jednej taśmie. Umożliwia to lepsze wykorzystanie szybkich napędów taśmowych. Domyślnie współczynnik

multipleksowania — czyli liczba agentów wysyłających dane na jedną taśmę — wynosi dwa. Można go zwiększyć do dziesięciu.

Multipleksowanie jest przydatne w dużych środowiskach, w których jest wykonywanych wiele operacji tworzenia kopii zapasowych. Nie poprawia to wydajności pojedynczych operacji tworzenia kopii zapasowych.

Aby uzyskać najszybsze tworzenie kopii zapasowych w dużym środowisku, należy przeanalizować przepustowość agentów, sieci i napędów taśmowych. Następnie należy odpowiednio ustawić współczynnik multipleksowania — unikając nadmiernego multipleksowania. Jeśli na przykład agenci dostarczają dane z szybkością 70 Mbit/s, napęd taśmowy zapisuje je z prędkością 250 Mbit/s, a w sieci nie ma wąskich gardeł, należy ustawić współczynnik multipleksowania na trzy. Współczynnik multipleksowania wynoszący cztery doprowadzi do nadmiernego multipleksowania i obniżenia wydajności tworzenia kopii zapasowych. Zazwyczaj współczynnik multipleksowania wynosi od dwóch do pięciu.

Ze względu na budowę multipleksowych kopii zapasowych są one wolniej odzyskiwane. Im wyższy współczynnik multipleksowania, tym wolniejsze odzyskiwanie. Jednoczesne odzyskiwanie wielu kopii zapasowych zapisanych na jednej multipleksowanej taśmie nie jest obsługiwane.

Możesz wybrać jeden lub więcej napędów taśmowych do multipleksowania lub skorzystać z opcji multipleksowania na dowolnym dostępnym napędzie taśmowym. Multipleksowanie jest niedostępne w przypadku lokalnie podłączonych napędów taśmowych.

Ustawień multipleksowania w istniejącym już planie ochrony nie można zmienić. Jeśli chcesz użyć innych ustawień, utwórz nowy plan ochrony.

W planie ochrony są możliwe następujące kombinacje wielu strumieni i multipleksowania:

- **Wyczyszczona zarówno opcja wielu strumieni, jak i opcja multipleksowania.**
  Każdy agent wysyła dane do jednego napędu taśmowego.
- **Zaznaczona tylko opcja wielu strumieni.**
  Każdy agent wysyła dane do co najmniej dwóch napędów taśmowych naraz.
- **Zaznaczona tylko opcja multipleksowania.**
  Każdy agent wysyła dane do napędu taśmowego przyjmującego strumienie od wielu agentów naraz. Maksymalna liczba strumieni, które może przyjąć napęd taśmowy, jest ustawiona w planie ochrony i nie można jej zmieniać w locie.
- **Zaznaczona zarówno opcja wielu strumieni, jak i opcja multipleksowania.**
  Każdy agent wysyła dane do co najmniej dwóch napędów taśmowych przyjmujących strumienie od wielu agentów naraz.

Napęd taśmowy może w danym czasie zapisywać tylko kopie zapasowe jednego rodzaju — multipleksowane lub niemultipleksowane — w zależności od tego, który plan ochrony został uruchomiony jako pierwszy.

Użyj zestawów taśm w ramach puli taśm wybranej na potrzeby kopii zapasowych

Ustawienie wstępne: **Wyłączono**.

Taśmy należące do jednej puli można grupować w postaci tak zwanych **zestawów taśm**.

Jeśli ta opcja pozostanie wyłączona, kopie zapasowe danych będą tworzone na wszystkich taśmach należących do puli. Jeśli ta opcja jest włączona, można rozdzielić kopie zapasowe zgodnie z wstępnie zdefiniowanymi lub niestandardowymi regułami.

- **Użyj osobnego zestawu taśm w każdym przypadku** (wybierz regułę: **Typ kopii zapasowej**, **Typ urządzenia**, **Nazwa urządzenia**, **Dzień miesiąca**, **Dzień tygodnia**, **Miesiąc roku**, **Rok**, **Data**).

  Jeśli jest wybrany ten wariant, można porządkować zestawy taśm według predefiniowanej reguły. Można na przykład używać oddzielnych zestawów taśm w każdym dniu tygodnia lub przechowywać kopie zapasowe poszczególnych komputerów na osobnych zestawach taśm.
- **Określ niestandardową regułę dla zestawów taśm**

  Jeśli jest wybrany ten wariant, należy określić własną regułę porządkowania zestawów taśm. Reguła może zawierać następujące zmienne:

Składnia zmiennej	Opis zmiennej	Wartości zmiennej
`[Resource Name]`	Kopie zapasowe poszczególnych komputerów są przechowywane na oddzielnych zestawach taśm.	Nazwy komputerów zarejestrowanych na serwerze zarządzania
`[Backup Type]`	Pełne, przyrostowe i różnicowe kopie zapasowe są przechowywane na oddzielnych zestawach taśm.	`full`, `inc`, `diff`
`[Resource Type]`	Kopie zapasowe komputerów poszczególnych typów są przechowywane na oddzielnych zestawach taśm.	`Server essentials`, `Server`, `Workstation`, `Physical machine`, `VMware Virtual Machine`, `Virtual-PC Virtual Machine`, `Virtual Server Virtual Machine`, `Hyper-V Virtual Machine`, `Parallels Virtual Machine`, `XEN Virtual Machine`, `KVM Virtual Machine`, `RHEV Virtual Machine`, `Parallels Cloud Virtual Machine`
`[Day]`	Kopie zapasowe utworzone w poszczególnych dniach miesiąca będą przechowywane na oddzielnych zestawach taśm.	`01`, `02`, `03`, ..., `31`

`[Weekday]`	Kopie zapasowe utworzone w poszczególnych dniach tygodnia będą przechowywane na oddzielnych zestawach taśm.	`Sunday`, `Monday`, `Tuesday`, `Wednesday`, `Thursday`, `Friday`, `Saturday`
`[Month]`	Kopie zapasowe utworzone w poszczególnych miesiącach roku będą przechowywane na oddzielnych zestawach taśm.	`January`, `February`, `March`, `April`, `May`, `June`, `July`, `August`, `September`, `October`, `November`, `December`
`[Year]`	Kopie zapasowe utworzone w poszczególnych latach będą przechowywane na oddzielnych zestawach taśm.	`2017`, `2018` itd.

- Jeśli na przykład zostanie określona reguła `[Resource Name]-[Backup Type]`, powstaną oddzielne zestawy taśm dla każdej pełnej, przyrostowej i różnicowej kopii zapasowej każdego komputera, do którego zastosowano plan ochrony.

Można też określić zestawy taśm dla poszczególnych taśm. W tym przypadku program najpierw zapisuje kopie zapasowe na taśmach, których wartość zestawu taśm odpowiada wartości wyrażenia określonego w planie ochrony. Następnie w razie potrzeby są używane inne taśmy z tej samej puli. W dalszej kolejności, jeśli pula jest uzupełniana, są używane taśmy z puli **wolnych taśm**.

Jeśli na przykład zostanie określony zestaw taśm `Monday` dla taśmy 1, `Tuesday` dla taśmy 2 itd., a następnie w opcjach tworzenia kopii zapasowej zostanie określona wartość `[Weekday]`, dla każdego dnia tygodnia będzie używana odpowiednia taśma.

Obsługa niepowodzenia zadania

Ta opcja określa zachowanie programu w sytuacji, gdy nie uda się wykonać planu ochrony zgodnie z harmonogramem. Nie jest ona uwzględniana, jeśli plan ochrony zostanie uruchomiony ręcznie.

W przypadku włączenia tej opcji program jeszcze raz spróbuje wykonać plan ochrony. 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: **Wyłączono**.

Warunki uruchomienia zadania

Ta opcja jest dostępna w systemach operacyjnych Windows i Linux.

Opcja określa działanie programu w sytuacji, gdy ma się rozpocząć jakieś zadanie (zbliża się zaplanowany termin lub wystąpiło zdarzenie określone w harmonogramie), ale warunek (lub jeden z wielu warunków) nie został spełniony. Aby uzyskać więcej informacji o warunkach, zobacz „Warunki rozpoczęcia”.

Ustawienie wstępne: **Poczekaj na spełnienie warunków z harmonogramu.**

Poczekaj na spełnienie warunków z harmonogramu

Przy tym ustawieniu funkcja harmonogramu rozpocznie monitorowanie warunków i uruchomi zadanie bezpośrednio po ich spełnieniu. Jeśli warunki nie zostaną w ogóle spełnione, zadanie nie zostanie uruchomione.

Jeśli warunki pozostają niespełnione przez zbyt długi czas i dalsze opóźnianie zadania staje się ryzykowne, można wyznaczyć czas, po upływie którego zadanie zostanie uruchomione niezależnie od warunku. Zaznacz pole wyboru **Uruchom zadanie mimo to po upływie** i podaj czas. Zadanie zostanie uruchomione niezwłocznie po spełnieniu warunków LUB po upływie maksymalnego czasu opóźnienia, w zależności od tego, która z tych sytuacji wystąpi wcześniej.

Pomiń wykonywanie zadania

Opóźnienie zadania może być niedopuszczalne, na przykład wtedy, gdy zadanie musi zostać wykonane dokładnie o określonej godzinie. Wówczas rozsądniej jest pominąć zadanie, zamiast czekać na spełnienie warunków, zwłaszcza w przypadku stosunkowo częstych zadań.

Usługa kopiowania woluminów w tle (VSS)

Ta opcja jest dostępna tylko w systemach operacyjnych Windows.

Określa ona, czy dostawca usługi kopiowania woluminów w tle (VSS) ma powiadamiać aplikacje uwzględniające usługę 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: **Włączono**. **Automatycznie wybierz dostawcę migawek**.

Można 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. 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.

Uwaga
Jeśli ta opcja jest włączona, nie jest tworzona kopia zapasowa plików i folderów określonych w kluczu rejestru **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\BackupRestore\FilesNotToSnapshot**. W szczególności dla plików danych offline programu Outlook (.ost) nie tworzy się kopii zapasowej, ponieważ są one określone w wartości **OutlookOST** tego klucza.

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.

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: **Włączono**.

W przypadku włączenia tej opcji transakcje wszystkich aplikacji uwzględniających usługę VSS działające na maszynie wirtualnej zostaną ukończone przed wykonaniem migawki. Jeśli po liczbie

prób określonej za pomocą opcji „Obsługa błędów” 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. Zaleca się niewyłączanie tej opcji nawet w przypadku maszyn wirtualnych, na których nie uruchamia się aplikacji obsługujących usługę VSS. W innym przypadku nie można zagwarantować integralności plików systemu wewnątrz zapisanej kopii zapasowej.

Uwaga
Ta opcja nie ma wpływu na maszyny wirtualne Scale Computing HC3. W ich przypadku wyciszenie zależy od tego, czy na maszynie wirtualnej są zainstalowane narzędzia Scale.

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**.

Dziennik zdarzeń systemu Windows

Ta opcja jest dostępna tylko w systemach operacyjnych Windows.

Ta 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: **Wyłączono**.

Odzyskiwanie

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 Przy użyciu nośnika startowego
Komputer fizyczny (z systemem Mac)	Przy użyciu nośnika startowego
Maszyna wirtualna (VMware, Hyper-V lub Scale Computing HC3)	Przy użyciu interfejsu internetowego Przy użyciu nośnika startowego
Konfiguracja ESXi	Przy użyciu nośnika startowego
Pliki/foldery	Przy użyciu interfejsu internetowego Pobieranie plików z chmury Przy użyciu nośnika startowego Wyodrębnianie plików z lokalnych kopii zapasowych
Stan systemu	Przy użyciu interfejsu internetowego
Bazy danych SQL	Przy użyciu interfejsu internetowego
Bazy danych programu Exchange	Przy użyciu interfejsu internetowego
Skrzynki pocztowe programu Exchange	Przy użyciu interfejsu internetowego
Skrzynki pocztowe Microsoft 365	Przy użyciu interfejsu internetowego
Bazy danych Oracle	Korzystanie z narzędzia Oracle Explorer

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.

Bezpieczne odzyskiwanie

Obraz systemu operacyjnego zapisany w kopii zapasowej może zostać zainfekowany złośliwym oprogramowaniem i może ponownie zainfekować komputer, na który jest odzyskiwany.

Funkcja bezpiecznego odzyskiwania umożliwia zapobieganie ponownej infekcji dzięki stosowaniu zintegrowanego skanowania antywirusowego oraz usuwaniu złośliwego oprogramowania podczas odzyskiwania.

Ograniczenia:

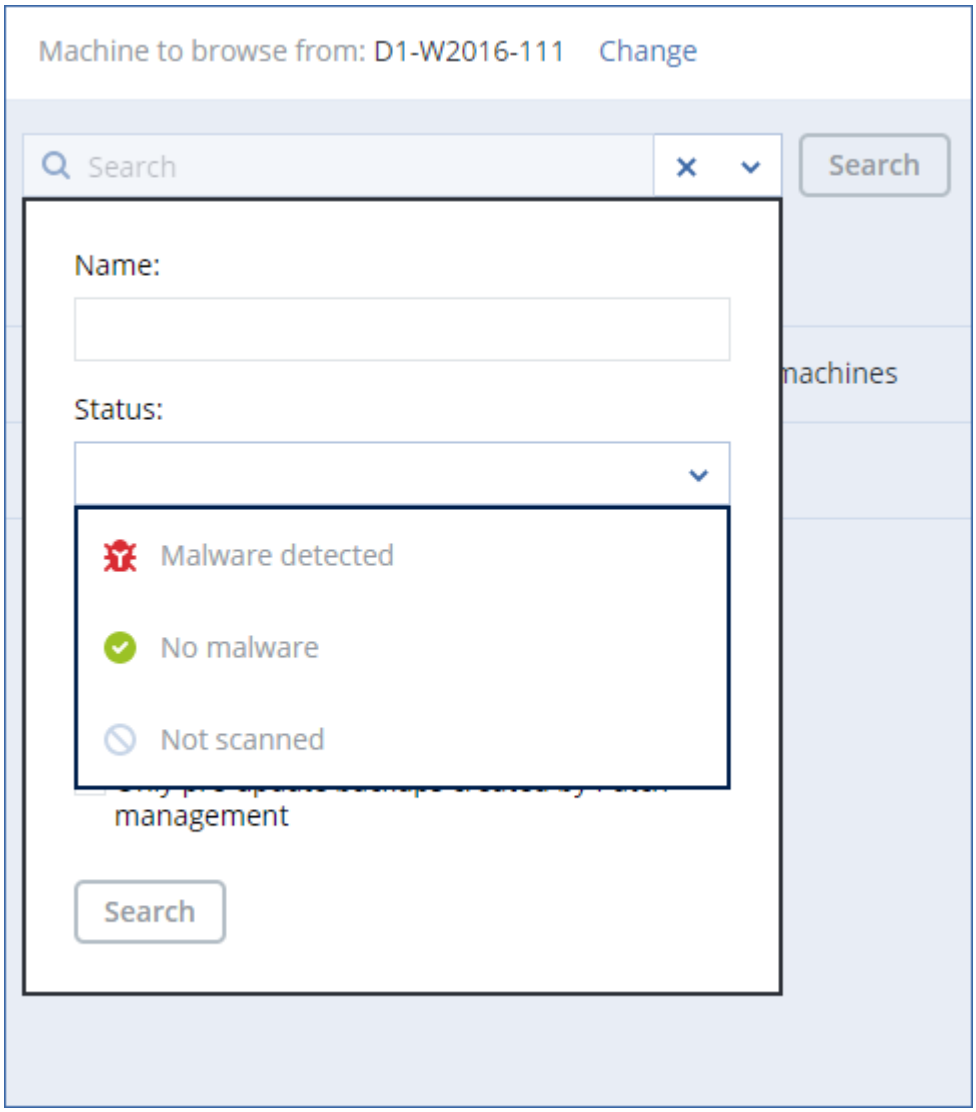
- Bezpieczne odzyskiwanie jest obsługiwane tylko w przypadku komputerów fizycznych lub maszyn wirtualnych z systemem Windows i zainstalowanym agentem dla systemu Windows.
- Obsługiwane są tylko kopie zapasowe typu **Cały komputer** lub **Dyski/woluminy**.
- Obsługiwane są tylko woluminy z systemem plików NTFS. Partycje z innym systemem plików zostaną odzyskane bez skanowania pod kątem złośliwego oprogramowania.
- Bezpieczne odzyskiwanie nie jest obsługiwane w przypadku kopii zapasowych objętych działaniem funkcji Ciągła ochrona danych (CDP). Komputer zostanie odzyskany przy użyciu ostatniej zwykłej kopii zapasowej — bez danych z kopii zapasowej CDP. Aby odzyskać dane z kopii zapasowej CDP, uruchom odzyskiwanie przy użyciu opcji **Pliki/foldery**.

Sposób działania

Jeśli podczas odzyskiwania zostanie włączona opcja Bezpieczne odzyskiwanie, system wykona następujące czynności:

1. Przeskanuje kopię zapasową obrazu w poszukiwaniu złośliwego oprogramowania i oznaczy zainfekowane pliki. Kopii zapasowej zostanie przypisany jeden z następujących statusów:
   - **Brak złośliwego oprogramowania** — oznacza, że podczas skanowania kopii zapasowej nie znaleziono złośliwego oprogramowania.
   - **Wykryto złośliwe oprogramowanie** — oznacza, że podczas skanowania kopii zapasowej znaleziono złośliwe oprogramowanie.
   - **Nie przeskanowano** — kopia zapasowa nie została przeskanowana pod kątem złośliwego oprogramowania.
2. Odzyska kopię zapasową na wybrany komputer.
3. Usunie wykryte złośliwe oprogramowanie.

Kopie zapasowe można filtrować przy użyciu parametru **Status**.



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 utworzyć nośnik po każdej ważnej aktualizacji agenta ochrony.

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

Aby utworzyć nośnik startowy w systemie Windows lub Linux

1. Pobierz plik ISO nośnika startowego. Aby pobrać plik, kliknij ikonę konta w prawym górnym rogu > **Do pobrania** > **Nośnik startowy**.
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.

  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.

Aby utworzyć nośnik startowy w systemie macOS

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 dysku zostaną skasowane.
3. Kliknij **Utwórz**.
4. Poczekaj, aż oprogramowanie utworzy nośnik startowy.

Odzyskiwanie komputera

Odzyskiwanie komputera fizycznego

W tej sekcji opisano procedurę odzyskiwania komputera fizycznego przy użyciu konsoli internetowej Cyber Protect.

Użyj nośnika startowego zamiast konsoli internetowej Cyber Protect, jeśli konieczne jest odzyskanie któregokolwiek z poniższych elementów:

- System operacyjny macOS
- Dowolny system operacyjny na komputer bez systemu operacyjnego lub komputer w trybie offline
- Struktura woluminów logicznych (woluminy utworzone przez narzędzie Logical Volume Manager w systemie Linux). Nośnik umożliwia automatyczne odtworzenie struktury woluminu logicznego.

Odzyskanie systemu operacyjnego i woluminów zaszyfrowanych przy użyciu funkcji BitLocker lub narzędzia CheckPoint wymaga ponownego uruchomienia systemu. Więcej informacji można znaleźć w sekcji "Odzyskiwanie z ponownym uruchomieniem" (s. 331).

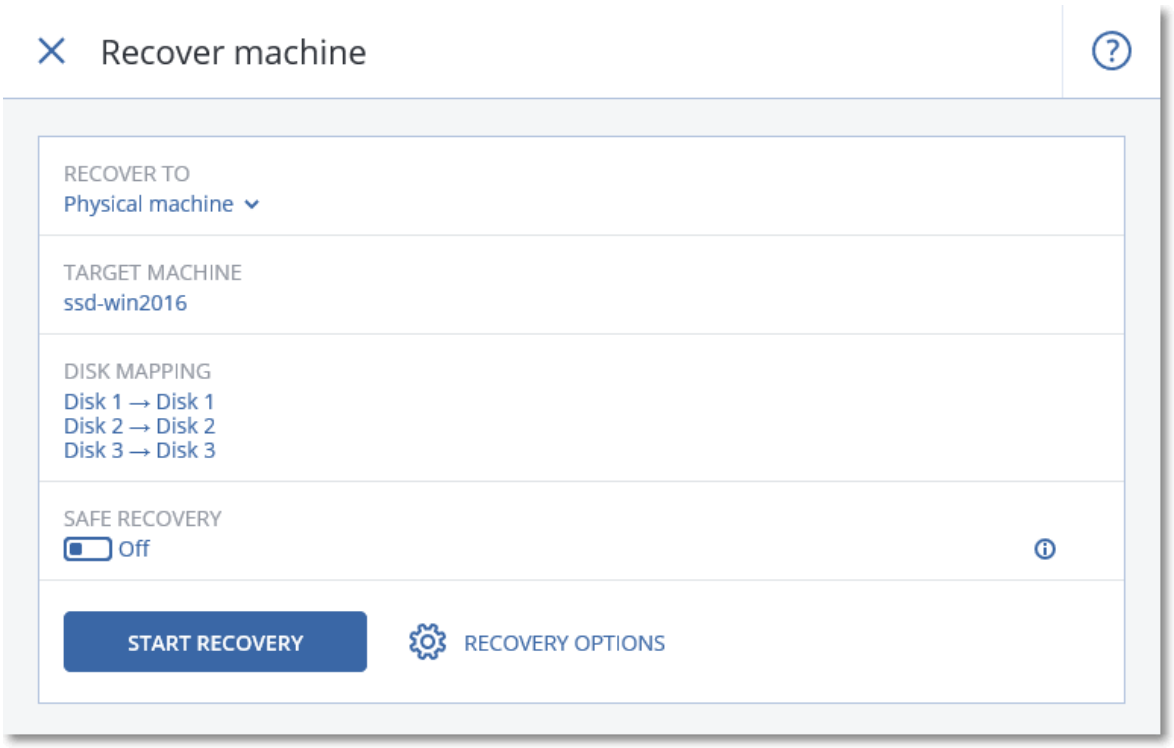
Aby odzyskać komputer fizyczny

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 Magazyn kopii zapasowych.
   - Odzyskaj komputer zgodnie z instrukcjami podanymi w sekcji „Odzyskiwanie dysków przy użyciu nośnika startowego”.
4. Kliknij **Odzyskaj** > **Cały komputer**.

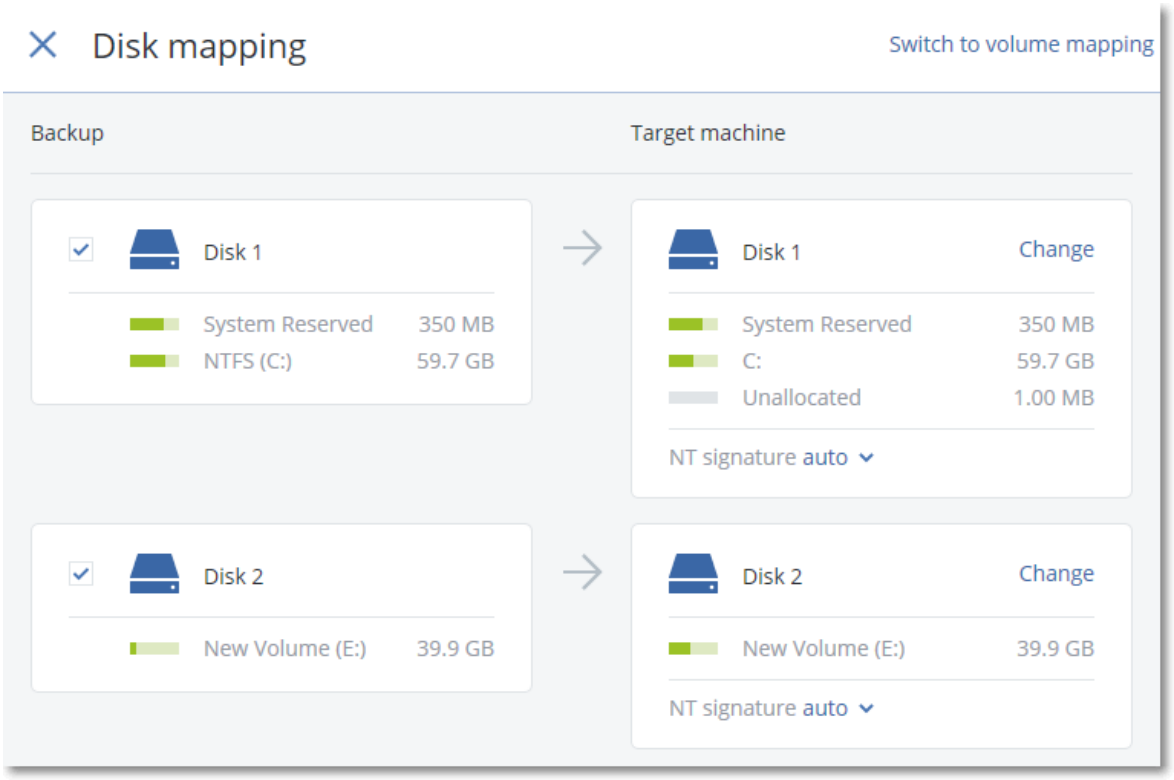
   Program automatycznie zamapuje dyski z kopii zapasowej na dyski komputera docelowego.

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



5. Jeśli mapowanie dysku się nie powiedzie lub będzie niezgodne z oczekiwaniami, kliknij opcję **Mapowanie dysków**, aby zamapować dyski ręcznie.

   Ponadto w sekcji mapowania można wybrać pojedyncze dyski lub woluminy do odzyskania. Możesz przełączać się między dyskami i woluminami do odzyskania przy użyciu linku **Przełącz na...** w prawym górnym rogu.



6. [Opcjonalnie] Włącz przełącznik **Bezpieczne odzyskiwanie**, aby przeskanować kopię zapasową pod kątem złośliwego oprogramowania. W przypadku wykrycia złośliwego oprogramowania zostanie ono oznaczone w kopii zapasowej i usunięte zaraz po zakończeniu odzyskiwania.
7. Kliknij **Rozpocznij odzyskiwanie**.
8. Potwierdź, że chcesz zastąpić dyski ich wersjami z kopii zapasowej. Określ, czy komputer ma zostać automatycznie ponownie uruchomiony.

Na karcie **Działania** jest wyświetlany postęp odzyskiwania.

Odzyskiwanie komputera fizycznego na maszynę wirtualną

Istnieje możliwość odzyskania kopii zapasowej komputera fizycznego na maszynę wirtualną.

Odzyskanie na maszynę wirtualną jest możliwe, jeśli w środowisku jest zainstalowany co najmniej jeden agent dla odpowiedniego docelowego hiperwizora i zarejestrowany na serwerze zarządzania. Na przykład odzyskanie do środowiska VMware ESXi wymaga, aby w środowisku był zainstalowany agent dla VMware i zarejestrowany na serwerze zarządzania.

Niektóre opcje są dostępne tylko w przypadku wdrożenia chmurowego.

Dodatkowe informacje na temat obsługiwanych ścieżek migracji komputera fizycznego na maszynę wirtualną (P2V) można znaleźć w sekcji "Migracja komputera" (s. 524).

Uwaga
Kopii zapasowych komputerów fizycznych z systemem macOS nie można odzyskiwać jako maszyn wirtualnych.

Aby odzyskać komputer fizyczny jako maszynę wirtualną

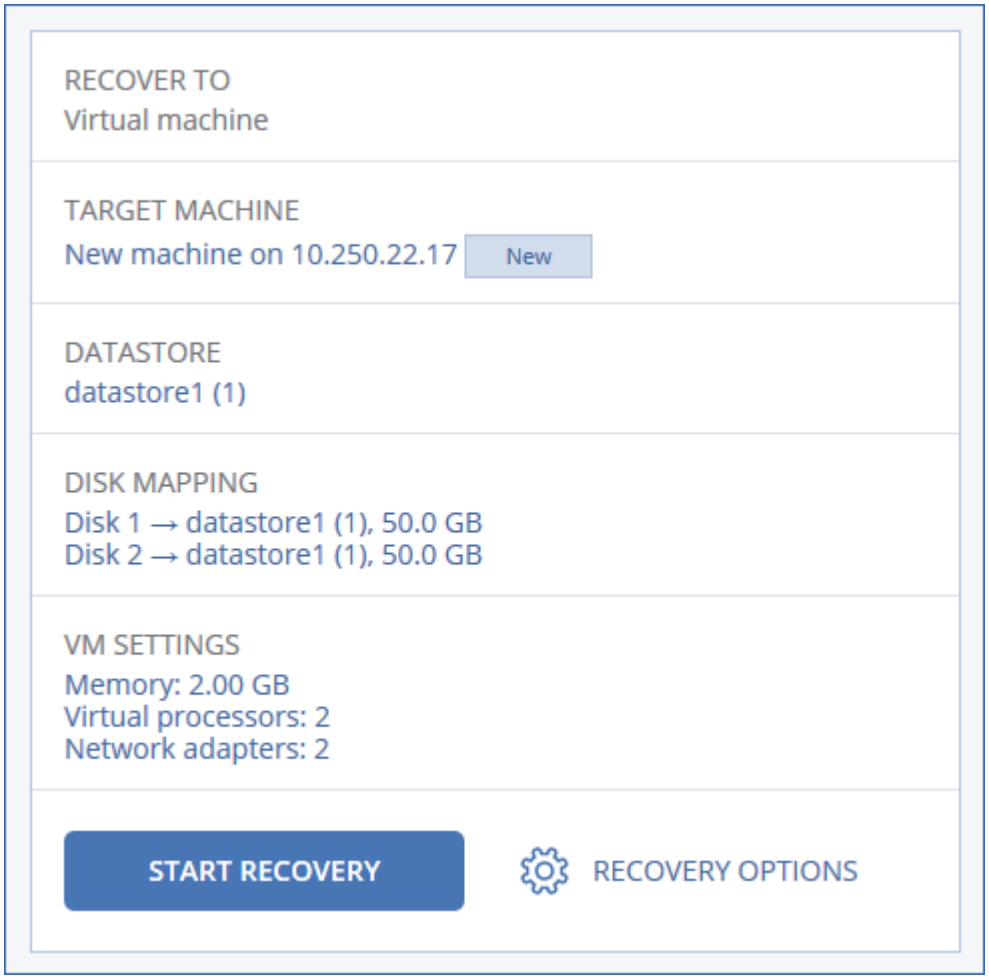
1. Wybierz komputer uwzględniony w kopii zapasowej.
2. Kliknij **Odzyskiwanie**.
3. Wybierz punkt odzyskiwania. Uwaga: punkty odzyskiwania są filtrowane na podstawie lokalizacji. Jeśli komputer jest w trybie offline, punkty odzyskiwania nie są wyświetlane. Wykonaj dowolne z następujących czynności:
   - Jeśli lokalizacją kopii zapasowych jest chmura lub magazyn współużytkowany (czyli taki, do którego mają dostęp inne agenty), kliknij **Wybierz komputer**, a następnie wybierz komputer będący w trybie online i punkt odzyskiwania.
   - Wybierz punkt odzyskiwania na karcie Magazyn kopii zapasowych.
   - Odzyskaj komputer zgodnie z opisem podanym w sekcji "Odzyskiwanie dysków i woluminów przy użyciu nośnika startowego" (s. 332).
4. Kliknij **Odzyskaj** > **Cały komputer**.
5. W polu **Odzyskaj do** wybierz **Maszyna wirtualna**.
6. Kliknij **Komputer docelowy**.
   a. Wybierz hiperwizor.

      Uwaga
      W środowisku musi być zainstalowany co najmniej jeden agent dla tego hiperwizora — i zarejestrowany na serwerze zarządzania.

   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. [W przypadku środowiska Virtuozzo Hybrid Infrastructure] Kliknij **Ustawienia maszyny wirtualnej**, a następnie wybierz **Wariant**. Opcjonalnie można zmienić rozmiar pamięci, liczbę procesorów oraz połączenia sieciowe maszyny wirtualnej.
8. [Opcjonalnie] [W przypadku odzyskiwania na nowy komputer] Skonfiguruj dodatkowe potrzebne opcje odzyskiwania:
   - [Możliwość niedostępna w przypadku środowisk Virtuozzo Hybrid Infrastructure i Scale Computing HC3] Aby wybrać magazyn danych dla maszyny wirtualnej, kliknij pozycję **Magazyn danych** w przypadku środowiska ESXi, **Ścieżka** w przypadku środowiska Hyper-V lub Virtuozzo lub **Domena magazynu** w przypadku środowiska Red Hat Virtualization (oVirt), a następnie wybierz magazyn danych (pamięć masową) dla maszyny wirtualnej.
   - Aby wybrać magazyn danych (pamięć masową), interfejs i tryb alokowania dla każdego dysku wirtualnego, kliknij **Mapowanie dysków**. W sekcji mapowania można wybrać pojedyncze dyski do odzyskania.

Uwaga
Tych ustawień nie można zmienić, jeśli odzyskujesz kontener Virtuozzo lub maszynę wirtualną Virtuozzo Hybrid Infrastructure. W przypadku środowiska Virtuozzo Hybrid Infrastructure możesz tylko wybrać zasady magazynowania dla dysków docelowych. W tym celu zaznacz żądany dysk docelowy, a następnie kliknij **Zmień**. W otwartym bloku kliknij ikonę koła zębatego, zaznacz zasady magazynowania, a następnie kliknij **Gotowe**.

- [Dostępne w przypadku środowisk VMware ESXi, Hyper-V, Virtuozzo i Red Hat Virtualization / oVirt] Kliknij **Ustawienia maszyny wirtualnej**, aby zmienić rozmiar pamięci, liczbę procesorów i połączenia sieciowe maszyny wirtualnej.



9. Kliknij **Rozpocznij odzyskiwanie**.
10. [W przypadku odzyskiwania na już istniejącą maszynę wirtualną] Potwierdź, że chcesz zastąpić dyski.

Na karcie **Działania** jest wyświetlany postęp odzyskiwania.

Odzyskiwanie maszyny wirtualnej

Kopię zapasową maszyny wirtualnej można odzyskać na komputer fizyczny lub inną maszynę wirtualną.

Odzyskanie na maszynę wirtualną jest możliwe, jeśli w środowisku jest zainstalowany co najmniej jeden agent dla odpowiedniego docelowego hiperwizora i zarejestrowany na serwerze zarządzania. Na przykład odzyskanie do środowiska VMware ESXi wymaga, aby w środowisku był zainstalowany agent dla VMware i zarejestrowany na serwerze zarządzania.

Niektóre opcje są dostępne tylko w przypadku wdrożenia chmurowego.

Dodatkowe informacje na temat obsługiwanych ścieżek migracji maszyny wirtualnej na komputer fizyczny (V2P) lub na maszynę wirtualną (V2V) można znaleźć w sekcji "Migracja komputera" (s. 524).

Uwaga
Nie można odzyskiwać maszyn wirtualnych macOS na hosty Hyper-V, ponieważ funkcja Hyper-V nie obsługuje systemu macOS. Maszyny wirtualne macOS można odzyskiwać na host VMware zainstalowany na sprzęcie Mac.

Ważne
Maszyna wirtualna musi zostać zatrzymana na czas odzyskiwania na inny komputer lub inną maszynę wirtualną. Domyślnie oprogramowanie zatrzyma maszynę bez wyświetlenia monitu. Po zakończeniu odzyskiwania trzeba będzie ręcznie uruchomić maszynę. To domyślne zachowanie można zmienić za pomocą opcji odzyskiwania służącej do zarządzania zasilaniem maszyn wirtualnych (kliknij **Opcje odzyskiwania** > **Zarządzanie zasilaniem maszyn wirtualnych**).

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 Magazyn kopii zapasowych.
2. Kliknij **Odzyskaj** > **Cały komputer**.
3. [W przypadku odzyskiwania na komputer fizyczny] W polu **Odzyskaj do** wybierz **Komputer fizyczny**.

   Odzyskanie na komputer fizyczny jest możliwe pod warunkiem, że konfiguracja dysków komputera docelowego jest dokładnie taka sama jak konfiguracja dysków w kopii zapasowej. W takim przypadku przejdź do kroku 4 w sekcji "Odzyskiwanie komputera fizycznego" (s. 324). W przeciwnym razie zalecamy przeprowadzenie migracji maszyny wirtualnej na komputer fizyczny (V2P) przy użyciu nośnika startowego.
4. [Opcjonalnie] Domyślnie pierwotny komputer jest wybierany jako komputer docelowy. Aby odzyskać na inną maszynę wirtualną, kliknij **Komputer docelowy**, a następnie wykonaj poniższe czynności:

a. Wybierz hiperwizor.

Uwaga
W środowisku musi być zainstalowany co najmniej jeden agent dla tego hiperwizora — i zarejestrowany na serwerze zarządzania.

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

c. Wybierz host, a następnie określ nazwę nowego komputera lub wybierz istniejący komputer docelowy.

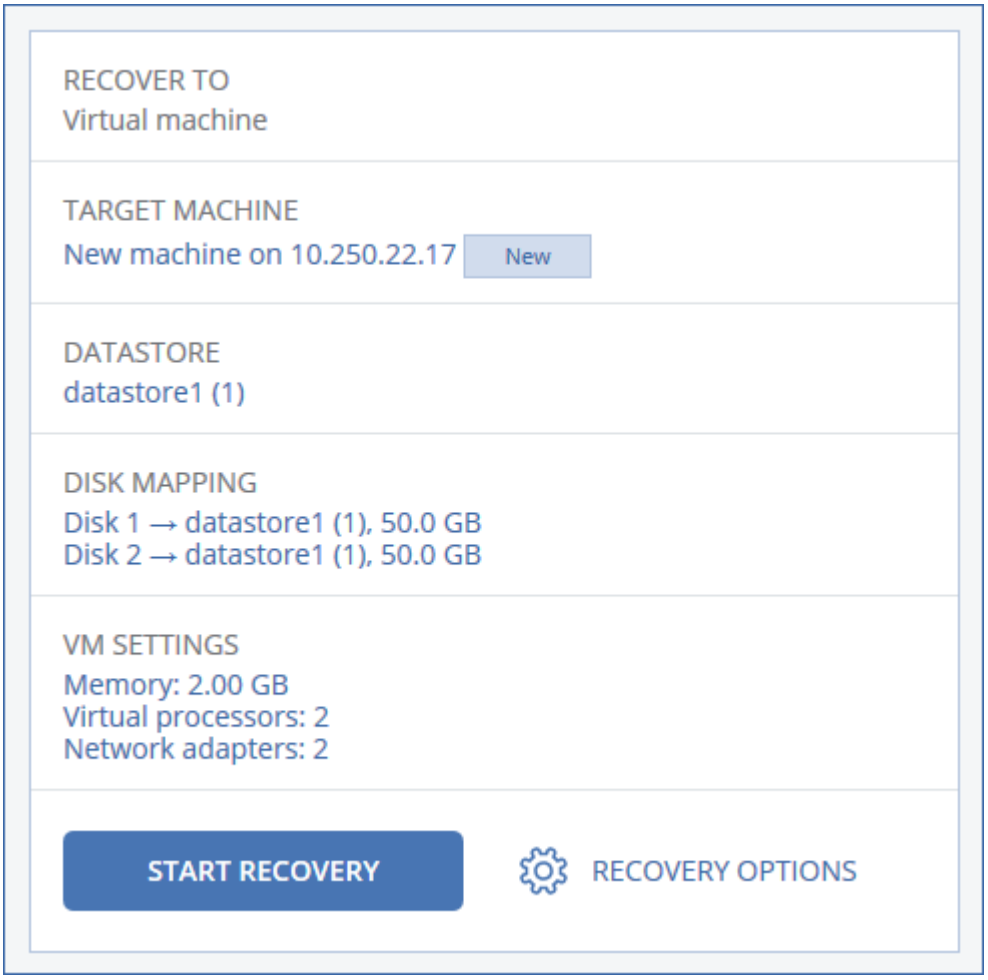
d. Kliknij **OK**.

5. [W przypadku środowiska Virtuozzo Hybrid Infrastructure] Kliknij **Ustawienia maszyny wirtualnej**, a następnie wybierz **Wariant**. Opcjonalnie można zmienić rozmiar pamięci, liczbę procesorów oraz połączenia sieciowe maszyny wirtualnej.
6. [Opcjonalnie] [W przypadku odzyskiwania na nowy komputer] Skonfiguruj dodatkowe potrzebne opcje odzyskiwania:
   - [Możliwość niedostępna w przypadku środowisk Virtuozzo Hybrid Infrastructure i Scale Computing HC3] Aby wybrać magazyn danych dla maszyny wirtualnej, kliknij pozycję **Magazyn danych** w przypadku środowiska ESXi, **Ścieżka** w przypadku środowiska Hyper-V lub Virtuozzo lub **Domena magazynu** w przypadku środowiska Red Hat Virtualization (oVirt), a następnie wybierz magazyn danych (pamięć masową) dla maszyny wirtualnej.
   - Aby wybrać magazyn danych (pamięć masową), interfejs i tryb alokowania dla każdego dysku wirtualnego, kliknij **Mapowanie dysków**. W sekcji mapowania można wybrać pojedyncze dyski do odzyskania.

     Uwaga
     Tych ustawień nie można zmienić, jeśli odzyskujesz kontener Virtuozzo lub maszynę wirtualną Virtuozzo Hybrid Infrastructure. W przypadku środowiska Virtuozzo Hybrid Infrastructure możesz tylko wybrać zasady magazynowania dla dysków docelowych. W tym celu zaznacz żądany dysk docelowy, a następnie kliknij **Zmień**. W otwartym bloku kliknij ikonę koła zębatego, zaznacz zasady magazynowania, a następnie kliknij **Gotowe**.

   - [Dostępne w przypadku środowisk VMware ESXi, Hyper-V, Virtuozzo i Red Hat Virtualization / oVirt] Kliknij **Ustawienia maszyny wirtualnej**, aby zmienić rozmiar pamięci, liczbę

procesorów i połączenia sieciowe maszyny wirtualnej.



7. Kliknij **Rozpocznij odzyskiwanie**.
8. [W przypadku odzyskiwania na już istniejącą maszynę wirtualną] Potwierdź, że chcesz zastąpić dyski.

Na karcie **Działania** jest wyświetlany postęp odzyskiwania.

Odzyskiwanie z ponownym uruchomieniem

Ponowne uruchomienie jest wymagane w przypadku odzyskiwania następujących elementów:

- System operacyjny
- Woluminy zaszyfrowane przy użyciu funkcji BitLocker lub narzędzia CheckPoint

Ważne
Zaszyfrowane woluminy z kopii zapasowej są odzyskiwane jako niezaszyfrowane.

Wymagania

- Odzyskanie zaszyfrowanych woluminów wymaga, by na tym samym komputerze znajdował się wolumin niezaszyfrowany i by było na nim co najmniej 1 GB wolnego miejsca. W przeciwnym

razie operacja odzyskiwania się nie powiedzie.

- Odzyskanie zaszyfrowanego woluminu systemowego nie wymaga żadnych dodatkowych czynności. Aby odzyskać zaszyfrowany wolumin niesystemowy, należy go najpierw zablokować, na przykład przez otwarcie pliku znajdującego się na tym woluminie. W przeciwnym razie odzyskiwanie będzie kontynuowane bez ponownego uruchomienia i odzyskany wolumin może nie zostać rozpoznany przez system Windows.

Rozwiązywanie problemów

Jeśli odzyskiwanie się nie powiedzie i komputer zostanie uruchomiony ponownie z komunikatem o błędzie `Nie można uzyskać pliku z partycji`, wyłącz funkcję Bezpieczny rozruch. Dodatkowe informacje o tym, jak to zrobić, można znaleźć w sekcji Wyłączanie funkcji Bezpieczny rozruch w dokumentacji firmy Microsoft.

Odzyskiwanie dysków i woluminów przy użyciu nośnika startowego

Informacje na temat tworzenia nośnika startowego można znaleźć w sekcji "Tworzenie nośnika startowego" (s. 323).

Aby odzyskać dyski lub woluminy przy użyciu nośnika startowego

1. Uruchom komputer docelowy, korzystając z nośnika startowego.
2. [Tylko w systemie macOS] W przypadku odzyskiwania woluminów sformatowanych przy użyciu systemu plików APFS na inny komputer niż pierwotny lub komputer bez systemu operacyjnego, należy ręcznie odtworzyć oryginalną konfigurację dysków:
   a. Kliknij **Narzędzie dyskowe**.
   b. Odtwórz oryginalną konfigurację dysków. Instrukcje można znaleźć w artykule https://support.apple.com/guide/disk-utility/welcome.
   c. Kliknij **Narzędzie dyskowe** > **Zamknij Narzędzie dyskowe**.

   Uwaga
   Począwszy od systemu macOS 11 Big Sur, nie można tworzyć kopii zapasowych ani odzyskiwać woluminów systemowych. Aby odzyskać możliwy do uruchomienia system macOS, należy odzyskać wolumin danych, a następnie zainstalować na nim system macOS.
3. Kliknij **Zarządzaj tym komputerem lokalnie** lub kliknij **Ratunkowy nośnik startowy** dwa razy, w zależności od typu używanego nośnika.
4. 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.
5. Na ekranie powitalnym kliknij **Odzyskaj**.
6. Kliknij **Wybierz dane**, a następnie kliknij **Przeglądaj**.

7. 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.
8. Wybierz kopię zapasową, z której chcesz odzyskać dane. Jeśli pojawi się monit, wpisz hasło kopii zapasowej.
9. W polu **Zawartość kopii zapasowej** wybierz **Dyski** lub **Woluminy**, a następnie wybierz elementy, które chcesz odzyskać. Kliknij **OK**, aby zatwierdzić wybór.

   Ważne
   Jeśli komputer uwzględniany w kopii zapasowej zawiera dyski dynamiczne lub woluminy logiczne (LVM), wybierz **Woluminy**.
10. 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.

    Uwaga
    Zmiana układu dysków może uniemożliwić uruchomienie systemu operacyjnego. Najlepiej użyć układu dysków pierwotnego komputera, chyba że ma się pewność udanej operacji.
11. [Tylko w przypadku systemu macOS] Aby odzyskać wolumin danych sformatowany w systemie APFS jako możliwy do uruchomienia system macOS, w **sekcji Instalacja systemu macOS** zachowaj zaznaczone pole wyboru **Zainstaluj system macOS na odzyskanym woluminie danych systemu macOS**.

    Po odzyskaniu danych system zostanie uruchomiony ponownie i automatycznie rozpocznie się instalacja systemu macOS. Instalator potrzebuje połączenia z Internetem, aby pobrać niezbędne pliki.

    Jeśli nie musisz odzyskiwać woluminu danych sformatowanego w systemie APFS jako możliwego do uruchomienia systemu, wyczyść pole wyboru **Zainstaluj system macOS na odzyskanym woluminie danych systemu macOS**. Wolumin można skonfigurować jako możliwy do uruchomienia później, ręcznie instalując na nim system macOS.
12. [Tylko w przypadku systemu Linux] Jeśli komputer uwzględniony w kopii zapasowej zawiera woluminy logiczne (LVM) 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**.
    c. Potwierdź wybór.

13. [Opcjonalnie] Kliknij **Opcje odzyskiwania**, aby określić dodatkowe ustawienia.
14. Kliknij **OK**, aby rozpocząć odzyskiwanie.

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.
5. Kliknij **OK**.

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.

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 adaptera sieciowego, a ścieżka do znalezionego sterownika jest przez nie następnie przekazywana 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.

Wskaż 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**.

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 ze wskazanych 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.

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.

Odzyskiwanie plików

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. Wykonaj jedną z następujących czynności:
   - [Zalecane] 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 Magazyn kopii zapasowych.
   - Pobierz pliki z magazynu chmurowego.
   - Użyj nośnika startowego.
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 „Filtry plików”.

   Uwaga
   W przypadku kopii zapasowych na poziomie dysku, które są przechowywanie w chmurze, wyszukiwanie jest niedostępne.
6. Wybierz pliki, które chcesz odzyskać.
7. Jeśli chcesz zapisać pliki jako plik .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 na tym komputerze jest zainstalowany agent).
   - Komputer z zainstalowanym agentem dla VMware, agentem dla Hyper-V lub agentem dla Scale Computing HC3 (jeśli pliki pochodzą z maszyny wirtualnej ESXi, Hyper-V lub Scale Computing HC3).

Jest to komputer docelowy operacji odzyskiwania. W razie potrzeby można wybrać inny komputer.

9. W polu **Ścieżka** wybierz miejsce docelowe odzyskiwania. Można wybrać jedną z następujących opcji:
   - Pierwotna lokalizacja (w przypadku odzyskiwania na pierwotny komputer)
   - Folder lokalny na komputerze docelowym

     Uwaga
     Łącza symboliczne nie są obsługiwane.

   - Folder sieciowy dostępny z komputera docelowego
10. Kliknij **Rozpocznij odzyskiwanie**.
11. Wybierz jedną z następujących opcji zastępowania plików:
    - **Zastąp istniejące pliki**
    - **Zastąp istniejący plik, jeśli jest starszy**
    - **Nie zastępuj istniejących plików**

Na karcie **Działania** jest wyświetlany postęp odzyskiwania.

Pobieranie plików z chmury

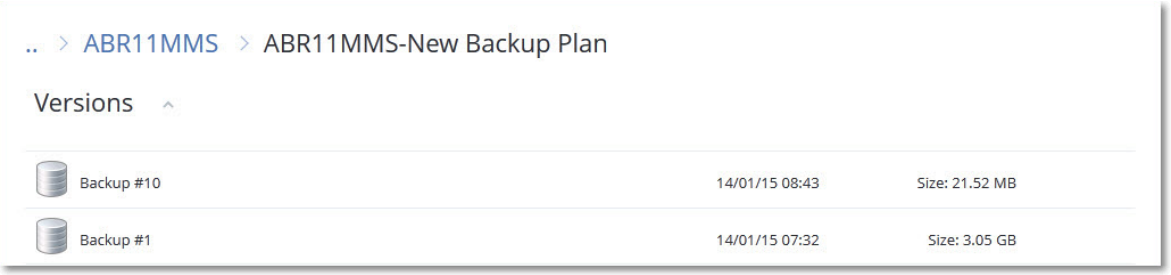
Można przeglądać chmurę, wyświetlać zawartość kopii zapasowych i pobierać potrzebne pliki.

Ograniczenia

- nie można przeglądać kopii zapasowych stanu systemu, baz danych SQL ani baz danych programu Exchange.
- Dla większego komfortu nie pobieraj jednocześnie więcej niż 100 MB. Aby szybko pobrać większą ilość danych z chmury, skorzystaj z procedury odzyskiwania plików.

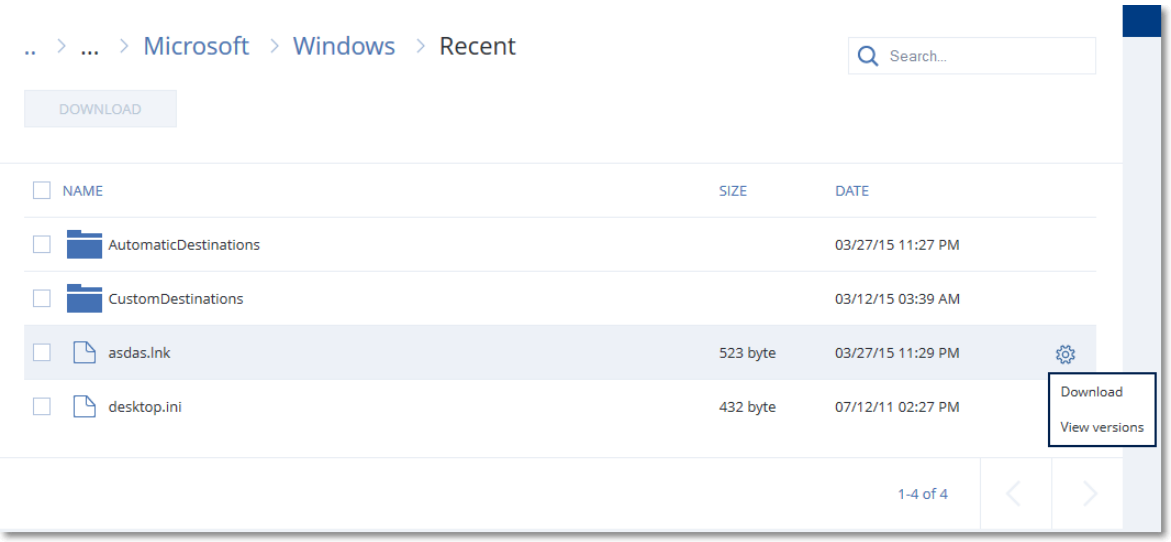
Aby pobrać pliki z chmury

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 sekcji **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 odpowiedniego folderu lub użyj funkcji wyszukiwania, aby uzyskać odpowiednią listę plików.



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**.

Weryfikowanie autentyczności pliku przy użyciu usługi Notary

Jeśli podczas tworzenia kopii zapasowej było włączone poświadczanie, istnieje możliwość weryfikacji autentyczności pliku uwzględnionego w kopii zapasowej.

Aby zweryfikować autentyczność pliku

1. Wybierz plik zgodnie z opisem podanym w krokach 1–6 sekcji „Odzyskiwanie plików przy użyciu interfejsu internetowego” lub w krokach 1–5 sekcji „Pobieranie plików z chmury”.
2. Sprawdź, czy wybrany plik jest oznaczony następującą ikoną:  . Oznacza to, że plik został notaryzowany.
3. Wykonaj jedną z następujących czynności:

- Kliknij opcję **Sprawdź**.
  Program sprawdza autentyczność pliku i wyświetla wynik.
- Kliknij opcję **Uzyskaj certyfikat**.
  Certyfikat potwierdzający notaryzację pliku zostanie otwarty w oknie przeglądarki internetowej. Okno to zawiera również instrukcje umożliwiające ręczną weryfikację autentyczności pliku.

Podpisywanie pliku w usłudze ASign

Usługa ASign umożliwia wielu osobom elektroniczne podpisanie pliku uwzględnionego w kopii zapasowej. Funkcja ta jest dostępna tylko w przypadku kopii zapasowych na poziomie plików przechowywanych w chmurze.

W danej chwili może być podpisana tylko jedna wersja pliku. Jeśli utworzono wiele kopii zapasowych pliku, należy wybrać wersję do podpisania — tylko ta wersja będzie podpisana.

Usługa ASign umożliwia na przykład podpisywanie elektroniczne następujących plików:

- Umowy wynajmu i dzierżawy
- Umowy sprzedaży
- Umowy zakupu zasobów
- Umowy pożyczek
- Potwierdzenia zgody
- Dokumenty finansowe
- Dokumenty ubezpieczenia
- Zrzeczenia odpowiedzialności
- Dokumenty opieki zdrowotnej
- Prace naukowe
- Certyfikaty autentyczności produktu
- Umowy o zachowaniu poufności
- Listy ofertowe
- Umowy o poufności
- Umowy wykonawców niezależnych

Podpisywanie wersji pliku

1. Wybierz plik zgodnie z opisem w krokach 1–6 sekcji Odzyskiwanie plików przy użyciu interfejsu internetowego.
2. Dopilnuj, aby w lewym panelu została wybrana poprawna data i godzina.
3. Kliknij opcję **Podpisz tę wersję pliku**.

4. Określ hasło do konta w chmurze, na którym jest przechowywana kopia zapasowa. Nazwa logowania konta jest wyświetlana w oknie monitu.

   Interfejs usługi ASign zostanie otwarty w oknie przeglądarki internetowej.
5. Dodaj inne osoby podpisujące, określając ich adresy e-mail. Po wysłaniu zaproszeń nie można dodawać ani usuwać osób podpisujących, więc upewnij się, że lista zawiera wszystkie osoby, których podpis jest wymagany.
6. Kliknij **Zaproś do podpisania**, aby wysłać zaproszenia do wszystkich osób podpisujących.

   Każda osoba podpisująca otrzymuje wiadomość e-mail z prośbą o podpisanie. Gdy plik podpiszą już wszystkie poproszone o to osoby, zostanie on znotaryzowany i podpisany przez usługę notaryzacji.

   Otrzymasz powiadomienia o podpisaniu pliku przez każdą z tych osób oraz o ukończeniu całego procesu. Aby uzyskać dostęp do strony internetowej usługi ASign, kliknij **Wyświetl szczegóły** w dowolnej otrzymanej wiadomości e-mail.
7. Po zakończeniu procesu przejdź do strony internetowej usługi ASign i kliknij **Get document** (Uzyskaj dokument), aby pobrać dokument PDF, który zawiera:
   - Strona Certyfikat podpisu zawiera zebrane podpisy.
   - Strona Ścieżka audytu zawiera historię działań: kiedy zaproszenie zostało wysłane do osób podpisujących, kiedy plik został podpisany przez poszczególne osoby itd.

Odzyskiwanie plików przy użyciu nośnika startowego

Informacje na temat tworzenia nośnika startowego można znaleźć w sekcji „Tworzenie nośnika startowego”.

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.

Uwaga
Lokalizacja taśmy zajmuje dużo miejsca i może się nie mieścić w pamięci RAM podczas ponownego skanowania i odzyskiwania przy użyciu nośnika startowego opartego na systemie Linux lub środowisku WinPE. W przypadku systemu Linux trzeba zamontować inną lokalizację, aby zapisać dane na dysku lub w udziale. Zobacz Acronis Cyber Backup Advanced: Changing the TapeLocation Folder (KB 27445) (Acronis Cyber Backup Advanced: zmienianie folderu lokalizacji taśmy). W przypadku środowiska Windows PE obecnie nie ma żadnego obejścia tego problemu.

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 ochrony.
- System plików w kopii zapasowej musi być jednym z następujących: FAT16, FAT32, NTFS, ReFS, Ext2, Ext3, Ext4, XFS lub HFS+.
- Kopia zapasowa musi być przechowywana w folderze lokalnym lub udziale sieciowym (SMB/CIFS).

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> – <GUID planu ochrony>`
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 dane z kopii zapasowej.
5. Przejdź do odpowiedniego folderu.
6. Skopiuj potrzebne pliki do dowolnego folderu w systemie plików.

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.

Na karcie **Działania** jest wyświetlany postęp odzyskiwania.

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”.

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. Na ekranie powitalnym kliknij **Odzyskaj**.
4. Kliknij **Wybierz dane**, a następnie kliknij **Przeglądaj**.
5. Określ lokalizację kopii zapasowej:
   - Przejdź do folderu w obszarze **Foldery lokalne** lub **Foldery sieciowe**.

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

10. 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**.
11. [Opcjonalnie] W polu **Mapowanie sieci** zmień wynik automatycznego mapowania przełączników wirtualnych dostępnych w kopii zapasowej na fizyczne karty sieciowe.
12. [Opcjonalnie] Kliknij **Opcje odzyskiwania**, aby określić dodatkowe ustawienia.
13. Kliknij **OK**, aby rozpocząć odzyskiwanie.

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, macOS 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	macOS	Nośnik startowy	ESXi, Hyper-V, Scale Computing HC3	Windows
Sprawdzanie poprawności kopii zapasowej	+	+	+	+	+	+	+	+	+
Tryb startowy	+	-	-	-	-	-	-	+	-

Data i godzina plików	-	-	-	+	+	+	+	-	-
Obsługa błędów	+	+	+	+	+	+	+	+	+
Wykluczenia plików	-	-	-	+	+	+	+	-	-
Flashback	+	+	+	-	-	-	-	+	-
Odzyskiwanie pełnej ścieżki	-	-	-	+	+	+	+	-	-
Punkty zamontowania	-	-	-	+	-	-	-	-	-
Wydajność	+	+	-	+	+	+	-	+	+
Polecenia poprzedzające/następujące	+	+	-	+	+	+	-	+	+
Zmiana identyfikatorów SID	+	-	-	-	-	-	-	-	-
Zarządzanie zasilaniem maszyn wirtualnych	-	-	-	-	-	-	-	+	-
"Zarządzanie taśmami" (s. 352) > Używaj dyskowej pamięci podręcznej, aby przyspieszyć odzyskiwanie	-	-	-	+	+	+	-	-	-
Dziennik zdarzeń systemu Windows	+	-	-	+	-	-	-	Tylko Hyper-V	+
Włączanie zasilania po odzyskaniu	-	-	-	-	-	-	+	-	-

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. Ta operacja jest wykonywana przez agenta ochrony.

Ustawienie wstępne: **Wyłączono**.

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.

Uwaga
Sprawdzanie poprawności jest dostępne w przypadku chmury znajdującej się w centrum danych firmy Acronis i udostępnianej przez partnerów firmy Acronis.

Tryb startowy

Ta opcja jest dostępna tylko w przypadku odzyskiwania komputera fizycznego lub maszyny wirtualnej z kopii zapasowej na poziomie dysku zawierającej system operacyjny Windows.

Opcja umożliwia wybranie trybu startowego (BIOS lub UEFI), którego system Windows użyje po zakończeniu operacji odzyskiwania. Jeśli tryb startowy pierwotnego komputera był inny od wybranego trybu startowego, oprogramowanie:

- Zainicjuje dysk, na który odzyskujesz wolumin systemowy, zgodnie z wybranym trybem startowym (MBR w przypadku systemu BIOS, GPT w przypadku systemu UEFI).
- Dostosuje ustawienia systemu operacyjnego Windows tak, aby mógł on zostać uruchomiony przy użyciu wybranego trybu startowego.

Ustawienie wstępne: **Tak jak na komputerze docelowym.**

Możesz wybrać jedną z poniższych opcji:

- **Tak jak na komputerze docelowym**
  Agent działający na komputerze docelowym wykrywa tryb startowy aktualnie używany przez system Windows i wprowadza stosowne zmiany.
  Jest to najbezpieczniejsza wartość, która automatycznie zapewnia możliwość uruchomienia systemu, chyba że mają zastosowanie poniższe ograniczenia. Ponieważ opcja **Tryb startowy** nie

jest dostępna w ramach nośnika startowego, agent na nośniku zawsze działa tak, jakby ta wartość była wybrana.

- **Tak jak na komputerze uwzględnionym w kopii zapasowej**

  Agent działający na komputerze docelowym odczytuje tryb startowy z kopii zapasowej i wprowadza stosowne zmiany. Ułatwia to odzyskanie systemu na innym komputerze, nawet jeśli ten komputer korzysta z innego trybu startowego, a następnie zamianę dysku w komputerze uwzględnionym w kopii zapasowej.
- **BIOS**

  Agent działający na komputerze docelowym odczytuje wprowadza stosowne zmiany, aby umożliwić użycie systemu BIOS.
- **UEFI**

  Agent działający na komputerze docelowym odczytuje wprowadza stosowne zmiany, aby umożliwić użycie systemu UEFI.

W przypadku zmiany tego ustawienia procedura mapowania dysków zostanie ponowiona. Może to potrwać jakiś czas.

Zalecenia

Jeśli trzeba przenieść system Windows między systemami UEFI i BIOS:

- Odzyskaj cały dysk, na którym znajduje się wolumin systemowy. Jeśli odzyskasz tylko wolumin systemowy na istniejącym woluminie, agent nie będzie w stanie prawidłowo zainicjować dysku docelowego.
- Pamiętaj, że system BIOS nie pozwala na stosowanie dysków o pojemności przekraczającej 2 TB.

Ograniczenia

- Przeniesienie między systemami UEFI i BIOS jest obsługiwane w następujących przypadkach:
  - 64-bitowe wersje systemów operacyjnych Windows, począwszy od systemu Windows 7
  - 64-bitowe wersje systemów operacyjnych Windows Server, począwszy od systemu Windows Server 2008 SP1
- Jeśli kopia zapasowa jest przechowywana na urządzeniu taśmowym, przeniesienie między systemami UEFI i BIOS nie jest obsługiwane.

Jeśli przeniesienie między systemami UEFI i BIOS nie jest obsługiwane, agent zachowuje się tak, jakby było wybrane ustawienie **Tak jak na komputerze uwzględnionym w kopii zapasowej**. Jeśli komputer docelowy obsługuje zarówno system UEFI, jak i BIOS, należy ręcznie włączyć tryb startowy odpowiadający pierwotnemu komputerowi. W przeciwnym razie system nie uruchomi się.

Data i godzina plików

Ta opcja jest dostępna tylko podczas odzyskiwania plików.

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: **Włączono**.

Obsługa błędów

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

W razie błędu spróbuj ponownie

Ustawienie wstępne: **Włączono. 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 cichy)

Ustawienie wstępne: **Wyłączono**.

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.

Zapisz informacje o systemie w razie niepowodzenia odzyskiwania z ponownym rozruchem

Ta opcja jest dostępna w przypadku odzyskiwania dysku lub woluminu na komputer fizyczny z systemem Windows lub Linux.

Ustawienie wstępne: **Wyłączono**.

Jeśli ta opcja jest włączona, można wskazać folder na dysku lokalnym (w tym w pamięci flash lub na dysku HDD podłączonym do komputera docelowego) lub w udziale sieciowym, w którym będą zapisywane dziennik, informacje o systemie i pliki zrzutów awaryjnych. Plik ten pomoże pracownikom pomocy technicznej w ustaleniu natury problemu.

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.

Zabezpieczenia na poziomie plików

Ta opcja jest dostępna podczas odzyskiwania plików z kopii zapasowych woluminów sformatowanych w systemie plików NTFS wykonanych na poziomie dysku i na poziomie plików.

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

Ustawienie wstępne: **Włączono**.

Można wybrać opcję odzyskania uprawnień lub dziedziczenia przez pliki uprawnień NTFS z folderu, do którego są odzyskiwane.

Flashback

Ta opcja jest dostępna w przypadku odzyskiwania dysków i woluminów na komputerach fizycznych oraz maszynach wirtualnych, z wyjątkiem komputerów Mac.

Jeśli ta opcja jest włączona, odzyskiwane są tylko różnice między danymi z kopii zapasowej a danymi dysku docelowego. Przyspiesza to odzyskiwanie danych na ten sam dysk, który został uwzględniony w kopii zapasowej, zwłaszcza jeśli układ woluminu dysku nie uległ zmianie. Dane są porównywane na poziomie bloków.

W przypadku komputerów fizycznych porównanie danych na poziomie bloków jest czasochłonne. Jeśli połączenie z magazynem kopii zapasowych jest szybkie, odzyskanie całego dysku potrwa krócej niż obliczenie różnic w danych. Dlatego opcję warto włączyć tylko wtedy, gdy połączenie z magazynem kopii zapasowych jest wolne (na przykład wtedy, gdy kopia zapasowa jest przechowywana w chmurze lub zdalnym folderze sieciowym).

W przypadku odzyskiwania komputera fizycznego ustawienie wstępne zależy od lokalizacji kopii zapasowej:

- Jeśli lokalizacją kopii zapasowej jest chmura, ustawienie wstępne jest następujące: **Włączono**.
- W przypadku innych lokalizacji kopii zapasowej stosowane jest następujące ustawienie wstępne: **Wyłączono**.

W przypadku odzyskiwania maszyny wirtualnej ustawienie wstępne jest następujące: **Włączono**.

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: **Wyłączono**.

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.

Ustawienie wstępne: **Wyłączono**.

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.

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.

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.

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 wybierz plik wsadowy. Program nie obsługuje poleceń interaktywnych, czyli wymagających wpisania tekstu przez użytkownika (na przykład „pause”).
3. W polu **Katalog roboczy** wpisz ścieżkę do katalogu, w którym ma zostać wykonane polecenie lub plik wsadowy.
4. W polu **Argumenty** w razie potrzeby podaj argumenty wykonania 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 zadanie odzyskiwania niepowodzeniem*	Wybrane	Niewybrane	Wybrane	Niewybrane
Nie przeprowadzaj odzyskiwania przed zakończeniem wykonywania polecenia	Wybrane	Wybrane	Niewybrane	Niewybrane
Wynik				
	Ustawienie wstępne Przeprowadź odzyskiwanie dopiero po pomyślnym wykonaniu	Przeprowadź odzyskiwanie po wykonaniu polecenia, niezależnie od tego, czy zakończyło się	N.d.	Przeprowadź odzyskiwanie równolegle z wykonywaniem polecenia i niezależnie od wyniku jego

	polecenia. Zakończ odzyskiwanie niepowodzeniem, jeśli wykonanie polecenia się nie powiodło.	powodzeniem, czy niepowodzeniem.		wykonania.

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

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 wybierz plik wsadowy.
3. W polu **Katalog roboczy** wpisz ścieżkę do katalogu, w którym ma zostać 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 na karcie **Działania**.
6. Kliknij **Gotowe**.

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

Zarządzanie taśmami

Zarządzanie taśmami oferuje następujące opcje odzyskiwania:

Używaj dyskowej pamięci podręcznej, aby przyspieszyć odzyskiwanie

Ustawienie wstępne: **Wyłączono**.

Stanowczo zalecamy korzystanie z opcji **Używaj dyskowej pamięci podręcznej, aby przyspieszyć odzyskiwanie** przy odzyskiwaniu plików z archiwum obrazu. W przeciwnym razie operacja przywracania może trwać znacznie dłużej. Dzięki tej opcji odczytywanie danych z taśm jest przeprowadzane sekwencjami, unikając przerw i przewijania.

Zmiana identyfikatorów SID

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

Ta opcja nie działa w przypadku odzyskiwania na maszynę wirtualną przy użyciu agenta dla VMware, agenta dla Hyper-V lub agenta dla Scale Computing HC3.

Ustawienie wstępne: **Wyłączono**.

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.

Zarządzanie zasilaniem maszyn wirtualnych

Te opcje są dostępne w przypadku odzyskiwania na maszynę wirtualną przy użyciu agenta dla VMware, agenta dla Hyper-V lub agenta dla Scale Computing HC3.

Przed uruchomieniem odzyskiwania wyłącz docelowe maszyny wirtualne

Ustawienie wstępne: **Włączono**.

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.

Włącz docelową maszynę wirtualną po zakończeniu odzyskiwania

Ustawienie wstępne: **Wyłączono**.

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.

Dziennik zdarzeń systemu Windows

Ta opcja jest dostępna tylko w systemach operacyjnych Windows.

Ta 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: **Wyłączono**.

Włączanie zasilania po odzyskaniu

Ta opcja jest dostępna podczas pracy z nośnikiem startowym.

Ustawienie wstępne: **Wyłączono**.

Opcja umożliwia rozruch komputera w odzyskanym systemie operacyjnym bez działania użytkownika.

Odzyskiwanie po awarii

Ta funkcja jest dostępna tylko w chmurowych wdrożeniach programu Acronis Cyber Protect.
Szczegółowy opis tej funkcji można znaleźć na stronie
https://www.acronis.com/support/documentation/DisasterRecovery/index.html#43224.html.

Operacje dotyczące kopii zapasowych

Karta Magazyn kopii zapasowych

Na karcie **Magazyn kopii zapasowych** 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 systemie Windows pliki kopii zapasowych dziedziczą uprawnienia dostępu z folderu nadrzędnego. Dlatego zalecamy ograniczenie uprawnień do odczytu w przypadku tego folderu.

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 **Magazyn kopii zapasowych** 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 ochrony są automatycznie dodawane na karcie **Magazyn kopii zapasowych**.Aby dodać folder niestandardowy (na przykład odłączane urządzenie USB) do listy lokalizacji kopii zapasowych, kliknij **Przeglądaj** i określ ścieżkę folderu.

Ostrzeżenie!
Nie próbuj edytować plików kopii zapasowych ręcznie, ponieważ może to poskutkować uszkodzeniem plików i bezużytecznością tych kopii zapasowych. Ponadto zalecamy tworzenie kopii zapasowych danych lub korzystanie z replikacji kopii zapasowych, a nie ręczne przenoszenie plików kopii zapasowych.

Aby wybrać punkt odzyskiwania na karcie Magazyn kopii zapasowych

1. Na karcie **Magazyn kopii zapasowych** 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 ochrony>`
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.

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.

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.

Zamontowanie woluminów w trybie do odczytu i zapisu umożliwia modyfikowanie zawartości kopii zapasowej, czyli zapisywanie, przenoszenie, tworzenie, usuwanie plików lub folderów i uruchamianie programów składających się z jednego pliku. W tym trybie oprogramowanie tworzy przyrostową kopię zapasową zawierającą zmiany wprowadzone w zawartości kopii zapasowej. Należy pamiętać, że żadna z późniejszych kopii zapasowych nie będzie uwzględniać tych zmian.

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.

Scenariusze użycia

- **Udostępnianie danych**
  Zamontowane woluminy można łatwo udostępniać przez sieć.
- **Rozwiązanie odzyskiwania z wykorzystaniem rezerwowej bazy danych**
  Zamontuj wolumin zawierający bazę danych SQL z komputera, który ostatnio uległ awarii. Umożliwi to dostęp do bazy danych do czasu odzyskania uszkodzonego komputera. Metody tej można też używać do odzyskiwania granularnego danych programu Microsoft SharePoint przy użyciu programu SharePoint Explorer.
- **Czyszczenie z wirusów w trybie offline**

Jeśli komputer jest zainfekowany, zamontuj jego kopię zapasową, oczyść ją za pomocą programu antywirusowego (lub znajdź ostatnią niezainfekowaną kopię zapasową), a następnie odzyskaj komputer z tej kopii.

- **Sprawdzanie pod kątem błędów**

  Jeśli odzyskanie ze zmianą rozmiaru woluminu się nie powiodło, przyczyną może być błąd w systemie plików w kopii zapasowej. Zamontuj kopię zapasową w trybie do odczytu i zapisu. Następnie sprawdź, czy w zamontowanym woluminie nie ma błędów, korzystając z polecenia **chkdsk /r**. Po naprawieniu błędów i utworzeniu nowej przyrostowej kopii zapasowej odzyskaj system z tej kopii.

Aby zamontować wolumin z kopii zapasowej

1. W Eksploratorze plików przejdź do lokalizacji kopii zapasowej.
2. Kliknij dwukrotnie plik kopii zapasowej. Domyślnie nazwy plików mają następującą strukturę:
   `<nazwa komputera> – <GUID planu ochrony>`
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.

   Uwaga
   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 jedną z następujących opcji:
   - **Zamontuj**

     Uwaga
     W trybie do odczytu/zapisu można zamontować tylko ostatnią kopię zapasową z archiwum (ciągu kopii zapasowych).

   - **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**.
4. Jeśli wolumin został zamontowany w trybie do odczytu i zapisu, a jego zawartość została zmodyfikowana, określ, czy ma zostać utworzona przyrostowa kopia zapasowa zawierające te zmiany. W przeciwnym razie pomiń ten krok.

   Oprogramowanie odmontuje wybrany wolumin.

Sprawdzanie poprawności kopii zapasowych

Sprawdzanie poprawności to operacja badająca, czy można odzyskać dane z kopii zapasowej. Więcej informacji na temat tej operacji można znaleźć w sekcji "Sprawdzanie poprawności" (s. 365).

Aby sprawdzić poprawność kopii zapasowej

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

   Jeśli obciążenie jest w trybie offline, punkty odzyskiwania nie są wyświetlane. Wykonaj dowolne z następujących czynności:
   - Jeśli lokalizacją kopii zapasowych jest chmura lub magazyn współużytkowany (czyli taki, do którego mają dostęp inne agenty), kliknij **Wybierz komputer**, a następnie wybierz obciążenie docelowe będące w trybie online i punkt odzyskiwania.
   - Wybierz punkt odzyskiwania na karcie Magazyn kopii zapasowych. Więcej informacji na temat dostępnych tam kopii zapasowych można znaleźć w sekcji "Karta Magazyn kopii zapasowych" (s. 356).
4. Kliknij ikonę koła zębatego, a następnie kliknij **Sprawdź poprawność**.
5. Wybierz agenta, który ma przeprowadzić sprawdzanie poprawności.
6. Wybierz metodę sprawdzania poprawności.
7. Jeśli kopia zapasowa jest zaszyfrowana, podaj hasło szyfrowania.
8. Kliknij **Rozpocznij**.

Eksportowanie kopii zapasowych

Operacja eksportu polega na utworzeniu we wskazanej lokalizacji samowystarczalnej kopii wybranej kopii zapasowej. Oryginalna kopia zapasowa pozostaje niezmieniona. Eksport umożliwia wyodrębnienie określonej kopii zapasowej z ciągu przyrostowych i różnicowych kopii zapasowych w celu szybkiego jej odzyskania, zapisania na nośniku wymiennym bądź odłączanym albo w innym celu.

Wynikiem operacji eksportu zawsze jest pełna kopia zapasowa. Jeśli zechcesz zreplikować cały ciąg kopii zapasowych do innej lokalizacji i zachować wiele punktów odzyskiwania, użyj planu replikacji kopii zapasowej.

Nazwa pliku wyeksportowanej kopii zapasowej zależy od wartości opcji formatu kopii zapasowej:

- W przypadku formatu **Wersja 12** z dowolnym schematem tworzenia kopii zapasowych nazwa pliku kopii zapasowej będzie taka sama jak nazwa oryginalnego pliku kopii zapasowej, z wyjątkiem kolejnego numeru. Jeśli do danej lokalizacji zostanie wyeksportowanych kilka kopii zapasowych z tego samego ciągu kopii zapasowych, do nazw ich plików — z wyjątkiem pierwszego — zostanie dodany czterocyfrowy kolejny numer.
- W przypadku formatu **Wersja 11** ze schematem tworzenia kopii zapasowych **Zawsze przyrostowa (jednoplikowa)** nazwa pliku kopii zapasowej będzie dokładnie taka sama jak nazwa pliku oryginalnej kopii zapasowej. Jeśli do danej lokalizacji zostanie wyeksportowanych kilka kopii zapasowych z tego samego ciągu kopii zapasowych, każda operacja eksportu spowoduje zastąpienie poprzednio wyeksportowanej kopii zapasowej.
- W przypadku formatu **Wersja 11** z innym schematem tworzenia kopii zapasowych nazwa pliku kopii zapasowej będzie taka sama jak nazwa oryginalnego pliku kopii zapasowej, z wyjątkiem sygnatury czasowej. Sygnatury czasowe wyeksportowanych kopii zapasowych odpowiadają czasowi wykonania eksportu.

Wyeksportowana kopia zapasowa dziedziczy ustawienia szyfrowania i hasło po oryginalnej kopii zapasowej. W przypadku eksportowania zaszyfrowanej kopii zapasowej trzeba podać hasło.

Aby wyeksportować kopię zapasową

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 Magazyn kopii zapasowych.
4. Kliknij ikonę koła zębatego, a następnie kliknij **Eksportuj**.
5. Wybierz agenta, który ma przeprowadzić eksport.
6. Jeśli kopia zapasowa jest zaszyfrowana, podaj hasło szyfrowania. W przeciwnym razie pomiń ten krok.
7. Określ miejsce docelowe eksportu.
8. Kliknij **Rozpocznij**.

Usuwanie kopii zapasowych

Ostrzeżenie!
W przypadku usunięcia kopii zapasowej wszystkie jej dane zostaną nieodwracalnie wymazane. Usuniętych danych nie będzie można odzyskać.

Aby usunąć kopie zapasowe komputera będącego w trybie online i dostępnego w konsoli internetowej Cyber Protect

1. Na karcie **Wszystkie urządzenia** wybierz 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, kliknij ikonę koła zębatego, a następnie kliknij **Usuń**.
   - Aby usunąć wszystkie kopie zapasowe w wybranej lokalizacji, kliknij **Usuń wszystko**.
5. Potwierdź decyzję.

Aby usunąć kopie zapasowe dowolnego komputera

1. Na karcie **Magazyn kopii zapasowych** 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 ochrony>`
2. Wybierz grupę.
3. Wykonaj jedną z następujących czynności:
   - Aby usunąć jedną kopię zapasową, kliknij **Pokaż kopie zapasowe**, zaznacz kopię do usunięcia, kliknij ikonę koła zębatego, a następnie kliknij **Usuń**.
   - Aby usunąć zaznaczoną grupę, kliknij **Usuń**.
4. Potwierdź decyzję.

Aby usunąć kopie zapasowe bezpośrednio z chmury

1. Zaloguj się do chmury zgodnie z opisem podanym w sekcji „Pobieranie plików z chmury”.
2. Kliknij nazwę komputera, którego kopie zapasowe chcesz usunąć.

   Oprogramowanie wyświetli co najmniej jedną grupę kopii zapasowych.
3. Kliknij ikonę koła zębatego odpowiadającą grupie kopii zapasowych, którą chcesz usunąć.
4. Kliknij **Usuń**.
5. Potwierdź operację.

Karta Plany

W przypadku licencji na wersję Advanced do zarządzania planami ochrony i innymi planami służy karta **Plany**.

Każda sekcja karty **Plany** zawiera wszystkie plany określonego typu. Są dostępne następujące sekcje:

- **Ochrona**
- **Skanowanie kopii zapasowych**
- **Replikacja kopii zapasowej**
- **Sprawdzanie poprawności**
- **Czyszczenie**
- **Konwersja na maszynę wirtualną**
- **Replikacja maszyny wirtualnej**
- **Nośnik startowy**. Ta sekcja zawiera plany ochrony, które utworzono dla komputerów uruchamianych z nośników startowych i które mogą być stosowane tylko do takich komputerów.

W każdej sekcji można tworzyć, edytować, wyłączać, włączać lub usuwać plan, rozpoczynać jego wykonywanie i monitorować stan jego wykonania.

Możliwości klonowania i zatrzymywania są dostępne tylko w przypadku planów ochrony. W odróżnieniu od zatrzymania tworzenia kopii zapasowych na karcie **Urządzenia** zatrzymanie planu ochrony spowoduje zatrzymanie operacji tworzenia kopii zapasowych na wszystkich urządzeniach, do których zastosowano dany plan. Jeśli czasy rozpoczęcia operacji tworzenia kopii zapasowej dla wielu urządzeń są rozłożone w czasie, zatrzymanie planu ochrony spowoduje zatrzymanie trwających operacji tworzenia kopii zapasowych lub uniemożliwi ich rozpoczęcie.

Można także wyeksportować plan do pliku i zaimportować wcześniej wyeksportowany plan.

Przetwarzanie danych poza hostem

Większość czynności stanowiących część planu ochrony, np. replikacja, sprawdzanie poprawności i stosowanie reguł przechowywania, jest wykonywanych przez agenta wykonującego kopię zapasową. Stanowi to dodatkowe obciążenie dla komputera, na których uruchomiony jest agent, nawet po zakończeniu procesu tworzenia kopii zapasowej.

Oddzielenie planów skanowania pod kątem złośliwego oprogramowania, replikacji, sprawdzania poprawności, czyszczenia i konwersji od planów ochrony zapewnia elastyczność:

- aby wybrać innych agentów do wykonania tych operacji;
- aby zaplanować te operacje na godziny poza szczytem w celu zminimalizowania zużycia przepustowości sieci;
- aby przełożyć te operacje na godziny poza działalnością biznesową, jeśli w planach nie ma skonfigurowania dedykowanego agenta.

Jeśli używasz węzła magazynowania, rozsądnie będzie zainstalować dedykowanego agenta na tym samym komputerze.

W odróżnieniu od planów tworzenia kopii zapasowych i replikacji maszyn wirtualnych, które korzystają z ustawień czasu komputerów obsługujących agenty, plany przetwarzania danych poza hostem działają zgodnie z ustawieniami czasu komputera pełniącego funkcję serwera zarządzania.

Plan skanowania kopii zapasowych

Obsługiwane lokalizacje

Kopie zapasowe można skanować w poszukiwaniu złośliwego oprogramowania w następujących lokalizacjach: **Chmura**, **Folder lokalny** i **Folder sieciowy**. Do **folderu lokalnego** ma dostęp tylko agent zainstalowany na skanowanym komputerze.

Więcej informacji na temat skanowania kopii zapasowych i związanych z nim ograniczeń można znaleźć w sekcji „Skanowanie antywirusowe kopii zapasowych".

Aby utworzyć plan skanowania kopii zapasowych

1. W konsoli internetowej Cyber Protect kliknij **Plany** > **Skanowanie kopii zapasowych**.
2. Kliknij **Utwórz plan**.
3. [Opcjonalnie] Aby zmienić nazwę planu, kliknij ikonę ołówka obok nazwy domyślnej.
4. Wybierz agenta skanowania.
5. Wybierz lokalizację kopii zapasowych lub konkretne kopie zapasowe do przeskanowania.
   Możesz zaznaczyć wiele lokalizacji kopii zapasowych naraz. Aby uwzględnić wiele pojedynczych kopii zapasowych w jednym planie, należy je dodać jedną po drugiej.
6. [W przypadku wybrania opcji **Chmura** lub **Folder sieciowy**] Jeśli pojawi się monit, podaj poświadczenia umożliwiające dostęp do magazynu kopii zapasowych.
7. [W przypadku wybrania zaszyfrowanej kopii zapasowej] Podaj hasło dostępu do kopii zapasowej. W przypadku wybrania skarbca lub wielu zaszyfrowanych kopii zapasowych można określić jedno hasło. Jeśli hasło jest niepoprawne w przypadku danej kopii zapasowej, zostanie wyświetlony alert. Skanowane będą tylko te kopie zapasowe, w których przypadku podano prawidłowe hasło.
8. Skonfiguruj harmonogram skanowania.
9. Gdy skończysz, kliknij **Utwórz**.

Zostanie utworzony plan skanowania kopii zapasowych.

Replikacja kopii zapasowej

Obsługiwane lokalizacje

W poniższej tabeli podsumowano lokalizacje kopii zapasowych obsługiwane przez plany replikacji kopii zapasowej.

Lokalizacja kopii zapasowej	Obsługiwana jako źródło	Obsługiwana jako miejsce docelowe
Chmura	+	+
Folder lokalny	+	+
Folder sieciowy	+	+
Folder NFS	–	–
Secure Zone	–	–
Serwery SFTP	–	–
Lokalizacja zarządzana*	+	+
Urządzenie taśmowe	–	+

* Sprawdź ograniczenia opisane w temacie "Uwagi dla użytkowników mających licencję zaawansowaną" (s. 266).

Aby utworzyć plan replikacji kopii zapasowych

1. Kliknij **Plany** > **Replikacja kopii zapasowej**.
2. Kliknij **Utwórz plan**.
   Program wyświetli szablon nowego planu.
3. [Opcjonalnie] Aby zmienić nazwę planu, kliknij nazwę domyślną.
4. Kliknij **Agent** i wybierz agenta, który ma wykonać replikację.
   Możesz wybrać dowolnego agenta mającego dostęp do źródłowej i docelowej lokalizacji kopii zapasowych.
5. Kliknij **Elementy do zreplikowania**, a następnie wybierz kopie zapasowe, które zostaną zreplikowane przy użyciu tego planu.
   Możesz przełączać między wybieraniem kopii zapasowych a wybieraniem całych lokalizacji przy użyciu przełącznika **Lokalizacje** / **Kopie zapasowe** w prawym górnym rogu.
   Jeśli wybrane kopie zapasowe są zaszyfrowane, wszystkie muszą używać tego samego hasła szyfrowania. W przypadku kopii zapasowych używających różnych haseł szyfrowania utwórz oddzielne plany.
6. Kliknij **Miejsce docelowe**, a następnie określ lokalizację docelową.

7. [Opcjonalnie] W obszarze **Jak przeprowadzić replikację** wybierz kopie zapasowe do replikacji. Można wybrać jedną z następujących opcji:
   - **Wszystkie kopie zapasowe** (domyślna)
   - **Tylko pełne kopie zapasowe**
   - **Tylko ostatnia kopia zapasowa**
8. [Opcjonalnie] Kliknij **Harmonogram**, a następnie zmień harmonogram.
9. [Opcjonalnie] Kliknij **Reguły przechowywania**, a następnie określ reguły przechowywania dotyczące danej lokalizacji docelowej zgodnie z opisem w sekcji „Reguły przechowywania”.
10. Jeśli kopie zapasowe wybrane w sekcji **Elementy do zreplikowania** są zaszyfrowane, włącz przełącznik **Hasło do kopii zapasowej**, a następnie podaj hasło szyfrowania. W przeciwnym razie pomiń ten krok.
11. [Opcjonalnie] Aby zmodyfikować opcje planu, kliknij ikonę koła zębatego.
12. Kliknij **Utwórz**.

Sprawdzanie poprawności

Sprawdzanie poprawności to operacja badająca, czy można odzyskać dane z kopii zapasowej.

Sprawdzanie poprawności lokalizacji kopii zapasowych obejmuje wszystkie kopie zapasowe przechowywane w tej lokalizacji.

Sposób działania

Plan sprawdzania poprawności oferuje dwie metody sprawdzania poprawności. W przypadku wybrania obu metod operacje będą wykonywane po kolei.

- **Obliczenie sumy kontrolnej każdego bloku danych zapisanego w kopii zapasowej**
  Więcej informacji na temat sprawdzania poprawności przez obliczenie sumy kontrolnej można znaleźć w sekcji „Sprawdzanie poprawności kopii zapasowych”.
- **Uruchomienie maszyny wirtualnej z kopii zapasowej**
  Ta metoda działa tylko w przypadku kopii zapasowych na poziomie dysku, które obejmują system operacyjny. Aby skorzystać z tej metody, potrzebny jest host ESXi lub Hyper-V oraz zarządzający nim agent ochrony (agent dla VMware lub agent dla Hyper-V).
  Agent uruchamia maszynę wirtualną z kopii zapasowej, a następnie nawiązuje połączenie z oprogramowaniem VMware Tools lub Hyper-V Heartbeat Service, aby sprawdzić, czy system operacyjny został prawidłowo uruchomiony. Jeśli nie uda się nawiązać połączenia, agent będzie próbował się połączyć co dwie minuty, łącznie pięć razy. Jeśli żadna z prób nie zakończy się pomyślnie, sprawdzenie poprawności się nie powiedzie.
  Niezależnie od liczby planów sprawdzania poprawności i kopii zapasowych, których poprawność jest sprawdzana, agent dokonujący sprawdzenia poprawności uruchamia maszyny wirtualne pojedynczo. Gdy tylko wynik sprawdzania poprawności będzie znany, agent usunie daną maszynę wirtualną i uruchomi następną.

W przypadku sprawdzenie poprawności się nie powiedzie, można sprawdzić szczegóły w sekcji **Działania** na karcie **Przegląd**.

Obsługiwane lokalizacje

W poniższej tabeli podsumowano lokalizacje kopii zapasowych obsługiwane przez plany sprawdzania poprawności.

Lokalizacja kopii zapasowej	Obliczanie sumy kontrolnej	Uruchamianie maszyny wirtualnej
Chmura	+	+
Folder lokalny	+	+
Folder sieciowy	+	+
Folder NFS	–	–
Secure Zone	–	–
Serwery SFTP	–	–
Lokalizacja zarządzana	+	+
Urządzenie taśmowe	+	–

Aby utworzyć nowy plan sprawdzania poprawności

1. Kliknij opcję **Plany** > **Sprawdzanie poprawności**.
2. Kliknij **Utwórz plan**.
   Program wyświetli szablon nowego planu.
3. [Opcjonalnie] Aby zmienić nazwę planu, kliknij nazwę domyślną.
4. Kliknij opcję **Agent** i wybierz agenta, który ma wykonać sprawdzanie poprawności.
   Aby przeprowadzić sprawdzanie poprawności przez uruchomienie maszyny wirtualnej z kopii zapasowej, należy wybrać agenta dla VMware lub agenta dla Hyper-V. W przeciwnym razie można wybrać dowolnego agenta zarejestrowanego na serwerze zarządzania i mającego dostęp do lokalizacji kopii zapasowej.
5. Kliknij **Elementy, których poprawność należy sprawdzić**, a następnie wybierz kopie zapasowe, których poprawność ma zostać sprawdzona przy użyciu tego planu.
   Możesz przełączać między wybieraniem kopii zapasowych a wybieraniem całych lokalizacji przy użyciu przełącznika **Lokalizacje** / **Kopie zapasowe** w prawym górnym rogu.
   Jeśli wybrane kopie zapasowe są zaszyfrowane, wszystkie muszą używać tego samego hasła szyfrowania. W przypadku kopii zapasowych używających różnych haseł szyfrowania utwórz oddzielne plany.
6. [Opcjonalnie] W sekcji **Elementy do sprawdzenia poprawności** wybierz kopie zapasowe, których poprawność ma być sprawdzana. Można wybrać jedną z następujących opcji:

- **Wszystkie kopie zapasowe**
- **Tylko ostatnia kopia zapasowa**

7. [Opcjonalnie] Kliknij **Jak sprawdzić poprawność**, a następnie wybierz dowolną z następujących metod:
   - **Weryfikacja sumy kontrolnej**
     Program obliczy sumę kontrolną każdego bloku danych zapisanego w kopii zapasowej.
   - **Uruchom jako maszynę wirtualną**
     Program uruchomi maszynę wirtualną z każdej kopii zapasowej.
8. Jeśli wybierzesz **Uruchom jako maszynę wirtualną**:
   a. Kliknij **Komputer docelowy**, a następnie wybierz typ maszyny wirtualnej (ESXi lub Hyper-V), hosta oraz szablon nazwy maszyny.
      Domyślna nazwa to **[Nazwa komputera]_sprawdzenie poprawności**.
   b. Kliknij opcję **Magazyn danych** w przypadku maszyny wirtualnej ESXi lub **Ścieżka** w przypadku maszyny wirtualnej Hyper-V, a następnie wybierz magazyn danych dla maszyny wirtualnej.
   c. [Opcjonalnie] Zmień tryb alokowania dysku.
      Ustawienie domyślne to **Elastyczne** dla VMware ESXi i **Powiększający się dynamicznie** dla Hyper-V.
   d. [Opcjonalnie] Kliknij **Ustawienia maszyny wirtualnej**, aby zmienić rozmiar pamięci oraz połączenia sieciowe maszyny wirtualnej.
      Domyślnie maszyna wirtualna *nie* jest podłączona do sieci, a wielkość pamięci maszyny wirtualnej jest równa wielkości pierwotnej maszyny.

   Uwaga
   Przełącznik **Puls maszyny wirtualnej** jest zawsze włączony, co pozwala zweryfikować status pulsu maszyny wirtualnej zgłaszany przez narzędzia hiperwizora w systemie operacyjnym gościa (VMware Tools lub Hyper-V Integration Services) przez uruchomienie maszyny wirtualnej z kopii zapasowej. Przełącznik ten został zaprojektowany na potrzeby przyszłych wersji, więc nie można się nim posłużyć.

9. [Opcjonalnie] Kliknij **Harmonogram**, a następnie zmień harmonogram.
10. Jeśli kopie zapasowe wybrane w sekcji **Elementy, których poprawność należy sprawdzić** są zaszyfrowane, włącz przełącznik **Hasło do kopii zapasowej**, a następnie podaj hasło szyfrowania. W przeciwnym razie pomiń ten krok.
11. [Opcjonalnie] Aby zmodyfikować opcje planu, kliknij ikonę koła zębatego.
12. Kliknij **Utwórz**.

Czyszczenie

Czyszczenie to operacja polegająca na usunięciu nieaktualnych kopii zapasowych zgodnie z regułami przechowywania.

Obsługiwane lokalizacje

Plany czyszczenia obejmują wszystkie lokalizacje kopii zapasowych, z wyjątkiem folderów NFS, serwerów SFTP i partycji Secure Zone.

Aby utworzyć nowy plan czyszczenia

1. Kliknij **Plany** > **Czyszczenie**.
2. Kliknij **Utwórz plan**.
   Program wyświetli szablon nowego planu.
3. [Opcjonalnie] Aby zmienić nazwę planu, kliknij nazwę domyślną.
4. Kliknij **Agent**, a następnie wybierz agenta, który wykona czyszczenie.
   Możesz wybrać dowolnego agenta mającego dostęp do danej lokalizacji kopii zapasowych.
5. Kliknij **Elementy do wyczyszczenia**, a następnie wybierz kopie zapasowe, które zostaną wyczyszczone przez ten plan.
   Możesz przełączać między wybieraniem kopii zapasowych a wybieraniem całych lokalizacji przy użyciu przełącznika **Lokalizacje** / **Kopie zapasowe** w prawym górnym rogu.
   Jeśli wybrane kopie zapasowe są zaszyfrowane, wszystkie muszą używać tego samego hasła szyfrowania. W przypadku kopii zapasowych używających różnych haseł szyfrowania utwórz oddzielne plany.
6. [Opcjonalnie] Kliknij **Harmonogram**, a następnie zmień harmonogram.
7. [Opcjonalnie] Kliknij **Reguły przechowywania**, a następnie określ reguły przechowywania zgodnie z opisem w sekcji „Reguły przechowywania”.
8. Jeśli kopie zapasowe wybrane w sekcji **Elementy do wyczyszczenia** są zaszyfrowane, włącz przełącznik **Hasło do kopii zapasowej**, a następnie podaj hasło szyfrowania. W przeciwnym razie pomiń ten krok.
9. [Opcjonalnie] Aby zmodyfikować opcje planu, kliknij ikonę koła zębatego.
10. Kliknij **Utwórz**.

Konwersja na maszynę wirtualną

Można utworzyć osobny plan konwersji na maszynę wirtualną i uruchomić go ręcznie lub według harmonogramu.

Informacje na temat wymagań wstępnych i ograniczeń zawiera sekcja „Co trzeba wiedzieć o konwersji”.

Aby utworzyć plan konwersji na maszynę wirtualną

1. Kliknij **Plany** > **Konwersja na maszynę wirtualną**.
2. Kliknij **Utwórz plan**.
   Program wyświetli szablon nowego planu.
3. [Opcjonalnie] Aby zmienić nazwę planu, kliknij nazwę domyślną.

4. W obszarze **Konwertuj na** wybierz typ docelowej maszyny wirtualnej. Można wybrać jedną z następujących opcji:
   - **VMware ESXi**
   - **Microsoft Hyper-V**
   - **Scale Computing HC3**
   - **VMware Workstation**
   - **Pliki VHDX**

   Uwaga
   W celu oszczędzania miejsca w pamięci masowej każda konwersja na pliki VHDX powoduje zastąpienie w lokalizacji docelowej plików VHDX utworzonych podczas poprzedniej konwersji.

5. Wykonaj jedną z następujących czynności:
   - [W przypadku maszyn VMware ESXi, Hyper-V i Scale Computing HC3] Kliknij **Host**, wybierz host docelowy, a następnie określ szablon nazw nowych maszyn.
   - [W przypadku maszyn wirtualnych innego typu] W polu **Ścieżka** wskaż miejsce zapisu oraz szablon nazw plików maszyn wirtualnych.

   Domyślna nazwa to **[Nazwa komputera]_skonwertowany**.
6. Kliknij **Agent** i wybierz agenta, który ma przeprowadzić konwersję.
7. Kliknij **Elementy do przekonwertowania** i wybierz kopie zapasowe, które zostaną przekonwertowane na maszyny wirtualne w ramach tego planu.

   Możesz przełączać między wybieraniem kopii zapasowych a wybieraniem całych lokalizacji przy użyciu przełącznika **Lokalizacje** / **Kopie zapasowe** w prawym górnym rogu.

   Jeśli wybrane kopie zapasowe są zaszyfrowane, wszystkie muszą używać tego samego hasła szyfrowania. W przypadku kopii zapasowych używających różnych haseł szyfrowania utwórz oddzielne plany.
8. [Tylko w przypadku maszyn VMware ESXi i Hyper-V] Kliknij **Magazyn danych** w przypadku maszyny ESXi lub **Ścieżka** w przypadku maszyny Hyper-V, a następnie wybierz magazyn danych (magazyn) dla maszyny wirtualnej.
9. [Tylko w przypadku maszyn wirtualnych VMware ESXi i Hyper-V] Wybierz tryb alokowania dysku. Ustawienie domyślne to **Elastyczne** dla VMware ESXi i **Powiększający się dynamicznie** dla Hyper-V.
10. [Opcjonalnie] [W przypadku maszyn wirtualnych VMware ESXi, Hyper-V Scale Computing HC3] Kliknij **Ustawienia maszyny wirtualnej**, aby zmienić rozmiar pamięci, liczbę procesorów lub połączenia sieciowe maszyny wirtualnej.
11. [Opcjonalnie] Kliknij **Harmonogram**, a następnie zmień harmonogram.
12. Jeśli kopie zapasowe wybrane w sekcji **Elementy do przekonwertowania** są zaszyfrowane, włącz przełącznik **Hasło do kopii zapasowej**, a następnie podaj hasło szyfrowania. W przeciwnym razie pomiń ten krok.
13. [Opcjonalnie] Aby zmodyfikować opcje planu, kliknij ikonę koła zębatego.

14. Kliknij **Utwórz**.

Nośnik startowy

Ważne
Niektóre funkcje opisane w tej sekcji są dostępne tylko w przypadku wdrożeń lokalnych.

Nośnik startowy

Nośnik startowy to nośnik fizyczny (płyta CD lub DVD, dysk flash USB albo inny nośnik wymienny obsługiwany jako urządzenie startowe przez system BIOS komputera), który umożliwia uruchomienie agenta ochrony w środowisku opartym na systemie Linux lub w środowisku preinstalacyjnym systemu Windows (WinPE) bez udziału systemu operacyjnego.

Najczęstsze zastosowanie nośnika startowego:

- odzyskanie systemu operacyjnego, którego nie można uruchomić;
- uzyskanie dostępu do ocalałych danych w uszkodzonym systemie i utworzenie ich kopii zapasowej;
- wdrożenie systemu operacyjnego na nowym sprzęcie;
- utworzenie woluminów standardowych lub dynamicznych na nowym sprzęcie;
- utworzenie kopii zapasowej „sektor po sektorze" dysku z nieobsługiwanym systemem plików;
- utworzenie w trybie offline kopii zapasowej dowolnych danych, których kopii zapasowej nie można utworzyć w trybie online, na przykład z powodu zablokowania danych przez uruchomioną aplikację lub ograniczeń dostępu.

Komputer można też uruchomić metodą uruchamiania sieciowego przy użyciu serwerów Acronis PXE Server, Windows Deployment Services (WDS) lub Remote Installation Services (RIS). Serwery te wraz z przesłanymi komponentami startowymi także można uważać za pewien rodzaj nośnika startowego. Za pomocą tego samego kreatora można utworzyć nośnik startowy bądź skonfigurować serwer PXE lub WDS/RIS.

Utworzyć nośnik startowy czy pobrać gotowy?

Za pomocą Generatora nośnika startowego można utworzyć własny nośnik startowy (oparty na systemie Linux lub środowisku WinPE) na potrzeby komputerów z systemem Windows, Linux lub macOS. Aby mieć w pełni funkcjonalny nośnik startowy, trzeba podać klucz licencyjny programu Acronis Cyber Protect. Bez tego klucza nośnik startowy będzie obsługiwać tylko operacje odzyskiwania.

Uwaga
Nośnik startowy nie obsługuje dysków hybrydowych.

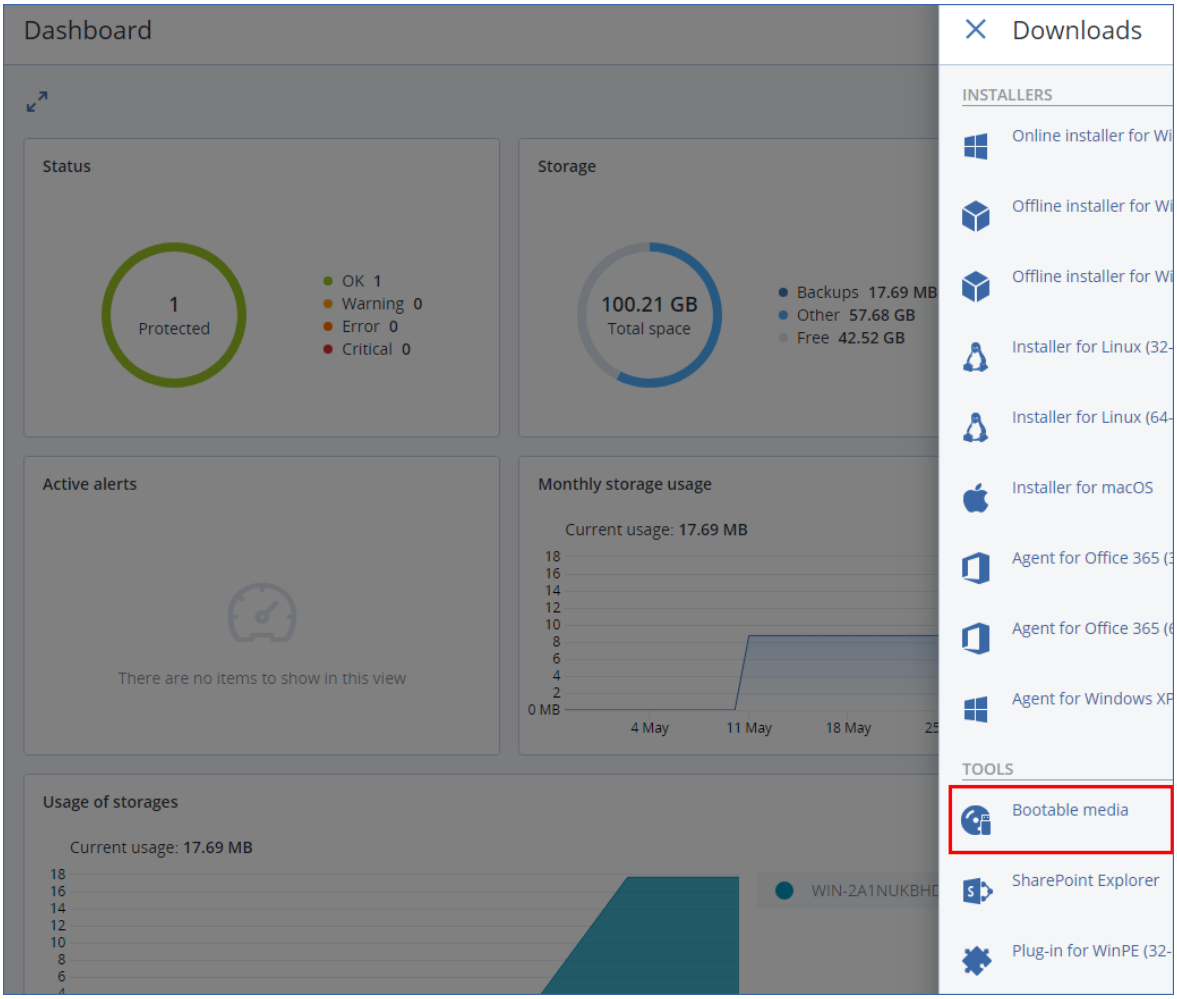
Można też pobrać gotowy nośnik startowy (tylko oparty na systemie Linux). Pobranego nośnika startowego można użyć tylko do operacji odzyskiwania i uzyskiwania dostępu do usługi Acronis

Universal Restore. Nie można tworzyć kopii zapasowych danych, sprawdzać poprawności i eksportować kopii zapasowych, zarządzać dyskami ani używać związanych z nośnikiem skryptów. Pobrany nośnik startowy nie nadaje się do komputerów z systemem macOS.

Uwaga
Gotowy nośnik startowy nie obsługuje węzła magazynowania, lokalizacji taśm ani lokalizacji SFTP. Aby korzystać z tych lokalizacji magazynów w ramach wdrożenia lokalnego, trzeba utworzyć własny nośnik startowy za pomocą Generatora nośnika startowego. Zobacz https://kb.acronis.com/content/61566.

Aby pobrać gotowy nośnik startowy

1. W konsoli internetowej Cyber Protect kliknij ikonę konta widoczną w prawym górnym rogu, a następnie kliknij **Do pobrania**.
2. Wybierz **Nośnik startowy**.



Możesz nagrać pobrany plik ISO na płytę CD/DVD lub utworzyć startowy dysk flash USB przy użyciu jednego z bezpłatnych narzędzi dostępnych online. Użyj narzędzia `ISO to USB` lub `RUFUS`, jeśli chcesz uruchomić komputer z systemem UEFI, albo narzędzia `Win32DiskImager` w przypadku komputera z systemem BIOS. W systemie Linux warto skorzystać z narzędzia `dd`.

Jeśli konsola internetowa Cyber Protect nie jest dostępna, możesz pobrać gotowy nośnik startowy z konta w portalu Acronis Customer Portal:

1. Otwórz stronę https://account.acronis.com.
2. Znajdź pozycję Acronis Cyber Protect i kliknij **Downloads** (Do pobrania).
3. Na otwartej stronie znajdź **Additional downloads** (Dodatkowe materiały do pobrania) i kliknij **Bootable Media ISO (for Windows and Linux)** (Obraz ISO nośnika startowego [dla systemu Windows i Linux]).

Nośnik startowy oparty na systemie Linux czy na środowisku WinPE?

opartym na systemie Linux

Nośnik startowy oparty na systemie Linux zawiera agenta ochrony opartego na jądrze systemu Linux. Agent może uruchamiać dowolny sprzęt klasy PC (w tym komputery bez systemu operacyjnego i komputery z uszkodzonymi lub nieobsługiwanymi systemami plików) oraz wykonywać na nim operacje. Operacje te można konfigurować i kontrolować lokalnie lub zdalnie w konsoli internetowej Cyber Protect.

Lista sprzętu obsługiwanego przez nośnik oparty na systemie Linux jest dostępna pod adresem: http://kb.acronis.com/content/55310.

Oparty na środowisku WinPE

Nośnik startowy oparty na środowisku WinPE zawiera minimalną wersję systemu Windows nazywaną środowiskiem preinstalacyjnym systemu Windows (WinPE) oraz wtyczkę programu Acronis do środowiska WinPE, czyli modyfikację agenta ochrony, która może działać w środowisku preinstalacyjnym.

Środowisko WinPE jest najwygodniejszym rozwiązaniem startowym w dużych środowiskach wyposażonych w różnorodny sprzęt.

Zalety:

- Korzystanie z programu Acronis Cyber Protect w środowisku preinstalacyjnym systemu Windows zapewnia więcej funkcji niż korzystanie z nośnika startowego opartego na systemie Linux. Po uruchomieniu sprzętu klasy PC w środowisku WinPE można używać nie tylko agenta ochrony, ale i poleceń oraz skryptów środowiska PE, a także innych wtyczek dodanych do tego środowiska.
- Nośnik startowy oparty na środowisku PE pozwala przezwyciężyć niektóre problemy z nośnikiem startowym związane z systemem Linux, takie jak obsługa tylko niektórych kontrolerów RAID lub niektórych poziomów macierzy RAID. Nośniki oparte na środowisku WinPE 2.x lub nowszym umożliwiają dynamiczne ładowanie potrzebnych sterowników urządzeń.

Ograniczenia:

- Nośniki startowe oparte na środowisku WinPE w wersji starszej niż 4.0 nie umożliwiają uruchamiania komputerów wykorzystujących technologię Unified Extensible Firmware Interface (UEFI).
- Gdy komputer uruchamiany jest z nośnika startowego ze środowiskiem PE, jako miejsca docelowego dla kopii zapasowej nie można wybrać nośnika optycznego, takiego jak płyta CD, DVD lub Blu-ray (BD).

Generator nośnika startowego

Generator nośnika startowego to specjalne narzędzie do tworzenia nośnika startowego. Jest dostępny tylko w przypadku 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.

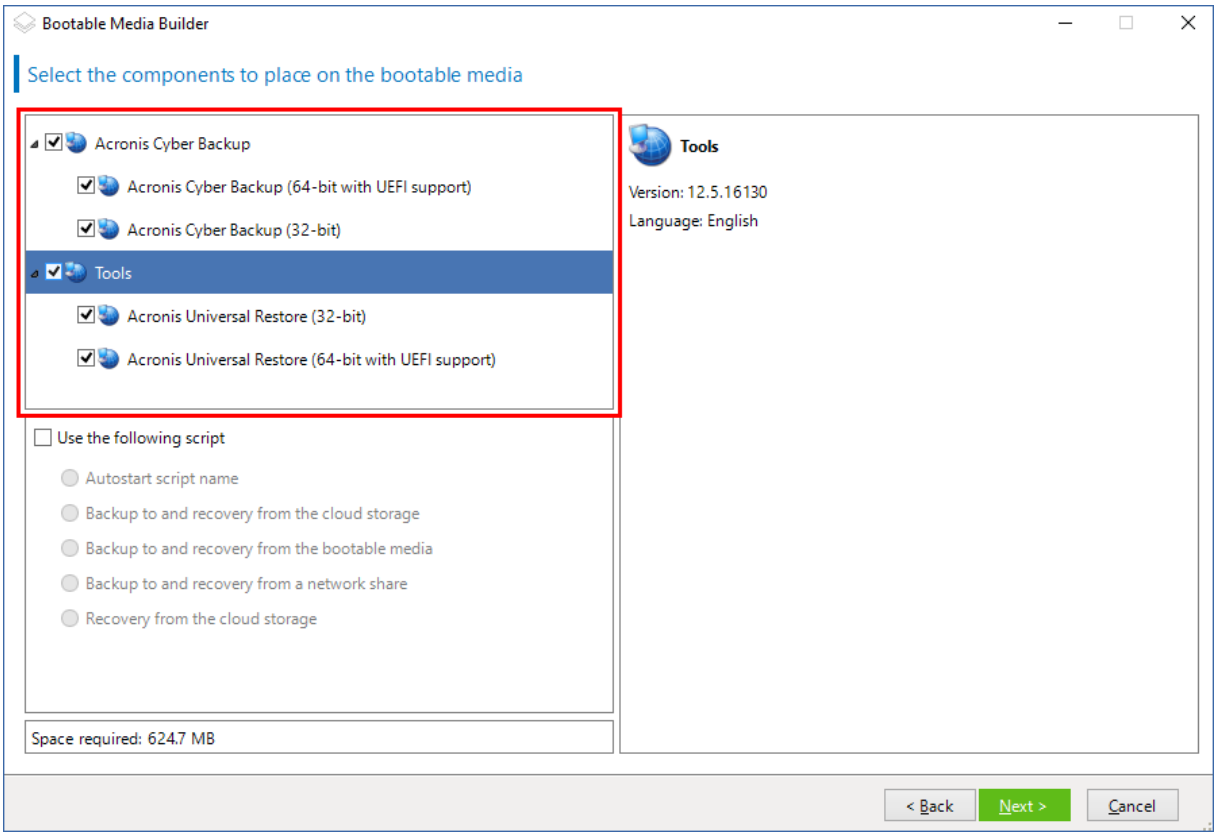
Dlaczego warto korzystać z generatora nośnika?

Gotowego nośnika startowego, który jest dostępny do pobrania w konsoli internetowej Cyber Protect, można używać tylko do 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, w pełni funkcjonalnego nośnika startowego opartego na systemie Linux lub środowisku WinPE obsługującego tworzenie kopii zapasowych.
- Oprócz utworzenia fizycznego nośnika startowego można przesłać jego komponenty do Usług wdrażania systemu Windows i skorzystać z funkcji uruchamiania sieciowego.
- Gotowy nośnik startowy nie obsługuje węzła magazynowania, lokalizacji taśm ani lokalizacji SFTP. Aby korzystać z tych lokalizacji magazynów w ramach wdrożenia lokalnego, trzeba utworzyć własny nośnik startowy za pomocą Generatora nośnika startowego. Zobacz https://kb.acronis.com/content/61566.

Wersja 32- czy 64-bitowa?

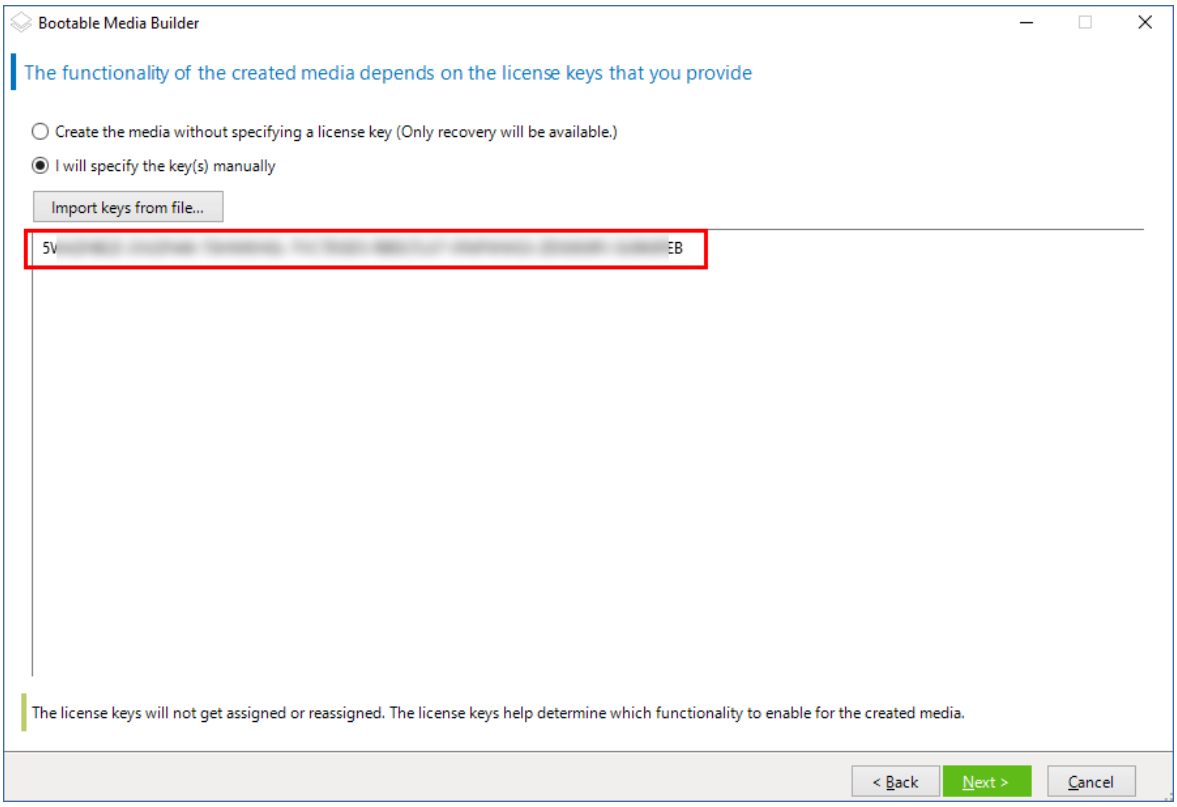
Generator nośnika startowego obsługuje tworzenie nośników z komponentami zarówno 32-, jak i 64-bitowymi. W większości przypadków do uruchomienia komputera korzystającego z interfejsu Unified Extensible Firmware Interface (UEFI) będzie potrzebny nośnik 64-bitowy.



Nośnik startowy oparty na systemie Linux

Aby utworzyć nośnik startowy oparty na systemie Linux

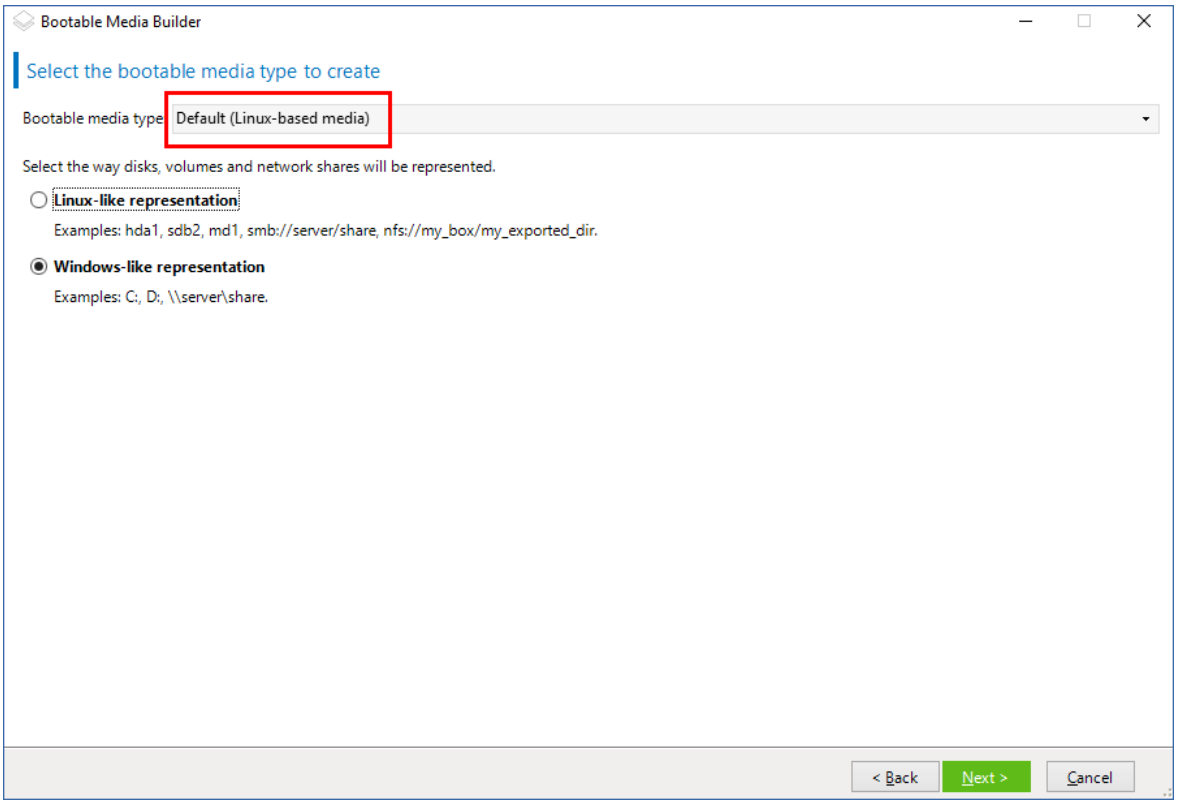
1. Uruchom **Generator nośnika startowego**.
2. Aby utworzyć w pełni funkcjonalny nośnik startowy, podaj klucz licencyjny programu Acronis Cyber Protect. Klucz ten posłuży do określenia, które funkcje zostaną uwzględnione na nośniku startowym. Żadna licencja nie zostanie odwołana z żadnego komputera.
   Jeśli nie podasz klucza licencyjnego, utworzonego nośnika startowego będzie można użyć tylko do operacji odzyskiwania.



3. Wybierz **Typ nośnika startowego: Domyślny (oparty na systemie Linux)**.

   Wybierz sposób reprezentacji woluminów i zasobów sieciowych:

   - W przypadku nośnika z reprezentacją woluminów w stylu systemu Linux są one wyświetlane na przykład jako hda1 i sdb2. Nośnik próbuje zrekonstruować urządzenia MD i woluminy logiczne (LVM) przed rozpoczęciem odzyskiwania.
   - W przypadku nośnika z reprezentacją woluminów w stylu systemu Windows są one wyświetlane na przykład jako C: i D:. Nośnik zapewnia dostęp do woluminów dynamicznych (LDM).



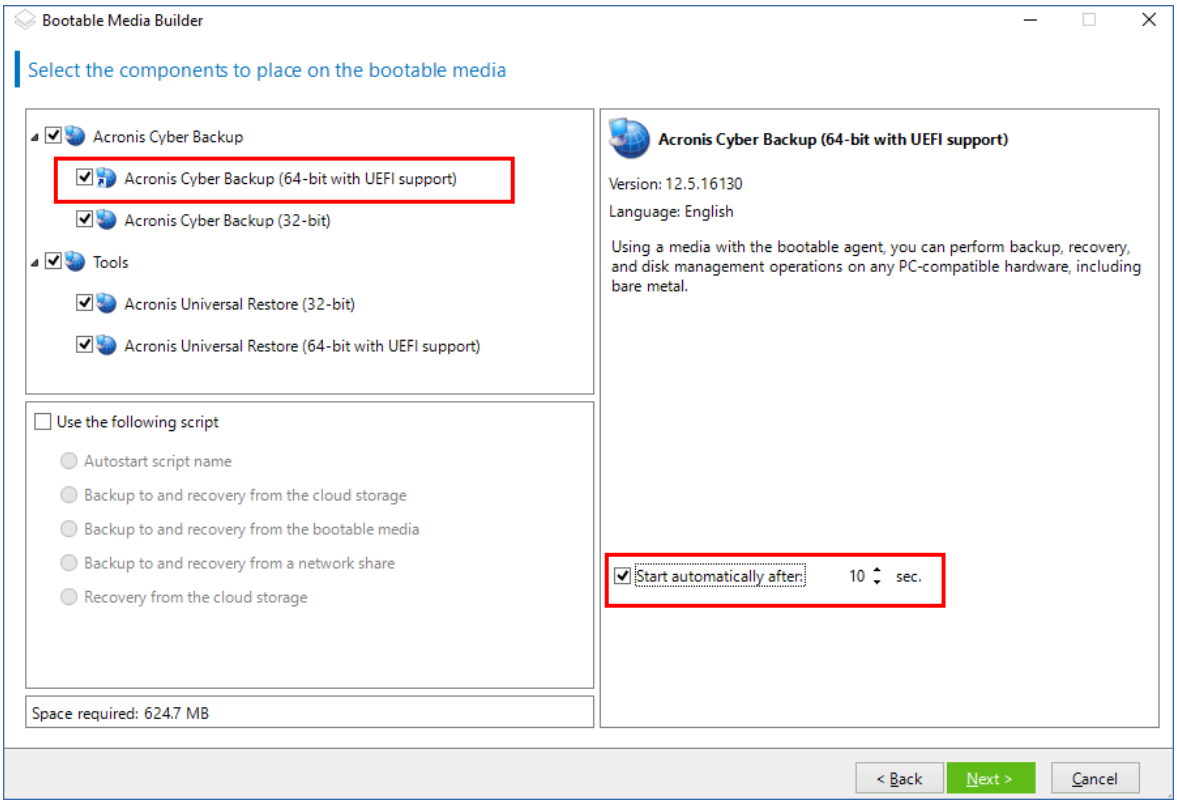
4. [Opcjonalnie] Określ parametry jądra systemu Linux. W przypadku wielu parametrów należy je rozdzielić spacjami.

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

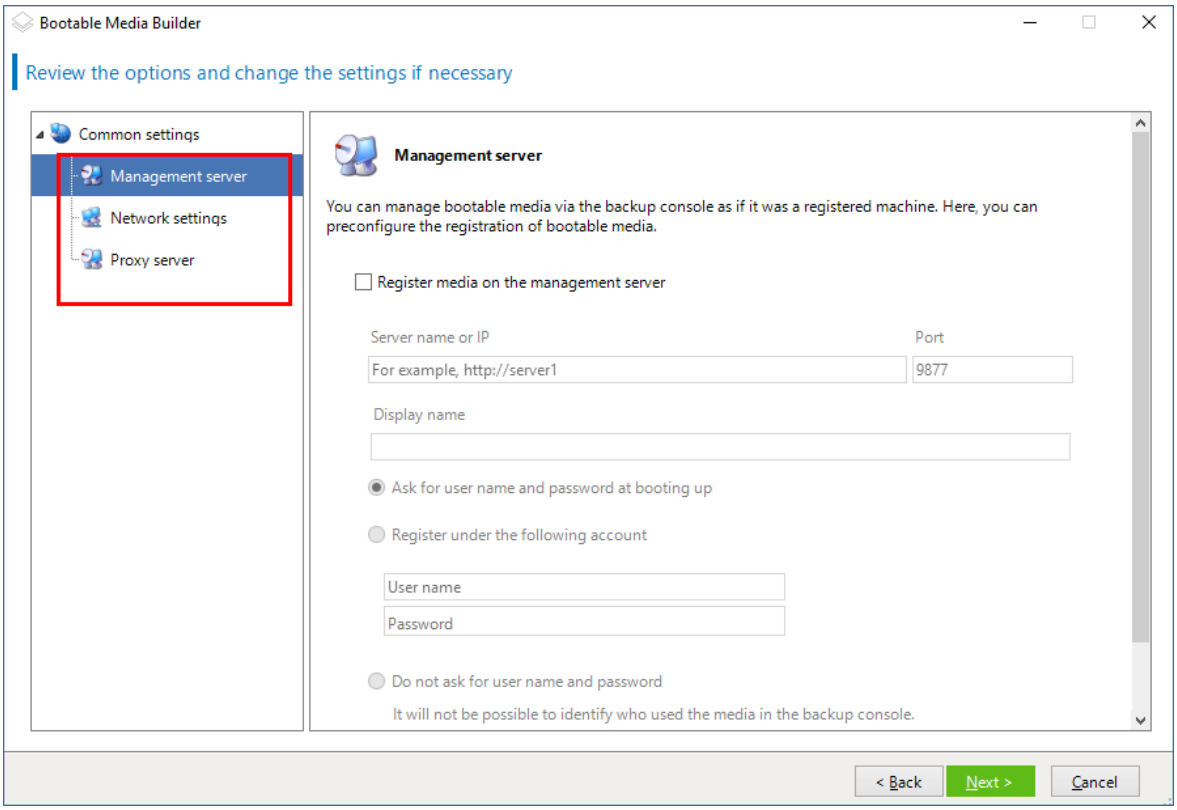
   Więcej informacji o dostępnych parametrach można znaleźć w sekcji Parametry jądra.
5. [Opcjonalnie] Wybierz język, który będzie używany na nośniku startowym.
6. Wybierz komponenty, które mają zostać umieszczone na nośniku: agent startowy programu Acronis Cyber Protect i/lub narzędzie Universal Restore, jeśli planujesz przywrócenie systemu na komputerze o innej konfiguracji sprzętowej.

   Agent startowy umożliwia wykonywanie operacji tworzenia kopii zapasowych i odzyskiwania oraz zarządzania dyskami, włącznie z odzyskiwaniem systemu po awarii, na dowolnym sprzęcie kompatybilnym ze standardem PC, w tym sprzęcie bez systemu operacyjnego.

   Narzędzie Universal Restore umożliwia uruchomienie systemu operacyjnego odzyskanego na komputer o innej konfiguracji sprzętowej lub maszynę wirtualną. Narzędzie to znajduje i instaluje sterowniki urządzeń, które mają zasadnicze znaczenie dla uruchomienia systemu operacyjnego, takie jak sterowniki kontrolerów pamięci masowej, płyty głównej czy chipsetu.
7. [Opcjonalnie] Określ limit czasu menu startowego oraz komponent uruchamiany automatycznie w przypadku przekroczenia tego limitu. W tym celu kliknij komponent w lewym górnym okienku, a następnie ustaw dla niego przedział czasowy. Umożliwia to wykonywanie na miejscu nienadzorowanej operacji w przypadku uruchamiania z serwera WDS/RIS.
   Jeśli to ustawienie nie jest skonfigurowane, program ładujący poczeka, aż zdecydujesz, czy ma zostać uruchomiony system operacyjny (jeśli jest dostępny), czy komponent.



8. [Opcjonalnie] Jeśli chcesz zautomatyzować operacje agenta startowego, zaznacz pole wyboru **Użyj następującego skryptu**. Następnie wybierz jeden ze skryptów i określ parametry skryptu.
9. [Opcjonalnie] Podczas uruchamiania wybierz sposób rejestracji nośnika na serwerze zarządzania. Aby uzyskać więcej informacji na temat ustawień rejestrowania, zobacz Serwer zarządzania.



10. [Opcjonalnie] Określ ustawienia sieciowe: Ustawienia TCP/IP, które zostaną przypisane do kart sieciowych komputera. Więcej informacji można znaleźć w sekcji "Ustawienia sieciowe" (s. 391).
11. [Opcjonalnie] Określ port sieciowy: Port TCP, na którym agent startowy nasłuchuje połączeń przychodzących.
12. [Opcjonalnie] Jeśli w sieci jest włączony serwer proxy, określ jego nazwę hosta / adres IP oraz port.
13. Wybierz typ nośnika. Użytkownik może:
    - Utwórz obraz ISO. Następnie możesz go nagrać na płytę CD/DVD, użyć do utworzenia startowego dysku flash USB lub podłączyć do maszyny wirtualnej.
    - Utwórz plik ZIP.
    - Przesłać wybrane komponenty na serwer Acronis PXE Server.
    - Przesłać wybrane komponenty na serwer WDS/RIS.
14. [Opcjonalnie] Dodać sterowniki przeznaczone do użycia przez narzędzie Universal Restore w systemie Windows. To okno jest wyświetlane, jeśli na nośniku umieszczono narzędzie Universal Restore i wybrano nośnik inny niż serwer WDS/RIS.
15. Jeśli pojawi się stosowny monit, określ nazwę hosta / adres IP oraz poświadczenia serwera WDS/RIS lub ścieżkę do pliku ISO nośnika.
16. Na ekranie podsumowania sprawdź ustawienia i kliknij **Kontynuuj**.

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 określany przez wartość *numer_trybu* podawaną 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**, warto najpierw użyć 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, w wierszu polecenia wpisz i uruchom polecenie **/bin/product**

nousb

Wyłącza ładowanie podsystemu obsługi interfejsu USB.

nousb2

Wyłącza obsługę interfejsu USB 2.0. Urządzenia USB 1.1 będą nadal obsługiwane. Przy użyciu tego parametru można użyć w trybie USB 1.1 tych dysków USB, które nie działają w trybie USB 2.0.

nodma

Wyłącza funkcję bezpośredniego dostępu do pamięci (DMA) dla wszystkich dysków twardych IDE. Zapobiega zawieszaniu się jądra przy niektórych urządzeniach

nofw

Wyłącz obsługę interfejsu FireWire (IEEE1394).

nopcmcia

Wyłącza rozpoznawanie urządzeń PCMCIA.

nomouse

Wyłącza obsługę myszy.

nazwa_modułu **=off**

Wyłącza moduł określony w parametrze *nazwa_modułu*. Aby na przykład wyłączyć obsługę modułu SATA, wpisz: **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.

LAYOUTS=en-US, de-DE, fr-FR, ...

Umożliwia określenie układów klawiatury, które mogą być używane w graficznym interfejsie użytkownika nośnika startowego.

W przypadku nieokreślenia tego parametru mogą być używane tylko dwa układy: Angielski (USA) oraz układ zgodny z językiem wybranym w menu startowym nośnika.

Można wskazać dowolny z następujących układów:

Belgijski: **be-BE**

Czeski: **cz-CZ**

Angielski: **en-GB**

Angielski (USA): **en-US**

Francuski: **fr-FR**

Francuski (szwajcarski): **fr-CH**

Niemiecki: **de-DE**

Niemiecki (szwajcarski): **de-CH**

Włoski: **it-IT**

Polski: **pl-PL**

Portugalski: **pt-PT**

Portugalski (brazylijski): **pt-BR**

Rosyjski: **ru-RU**

Serbski (cyrylica): **sr-CR**

Serbski (łaciński): **sr-LT**

Hiszpański: **es-ES**

Podczas pracy z nośnikiem startowym możesz przechodzić między dostępnych układami przy użyciu kombinacji klawisz CTRL + SHIFT.

Skrypty na nośniku startowym

Jeśli chcesz, aby nośnik startowy wykonywał ustalony zestaw operacji, możesz określić skrypt podczas tworzenia nośnika w generatorze nośnika startowego. Przy każdym uruchomieniu nośnik będzie uruchamiał ten skrypt zamiast wyświetlania interfejsu użytkownika.

Program pozwala wybrać jeden ze wstępnie zdefiniowanych skryptów lub utworzyć skrypt niestandardowy zgodnie z konwencjami dotyczącymi skryptów.

Wstępnie zdefiniowane skrypty

Generator nośnika startowego zapewnia następujące wstępnie zdefiniowane skrypty:

- Tworzenie kopii zapasowej w magazynie w chmurze i odzyskiwanie jej (**entire_pc_cloud**)
- Tworzenie kopii zapasowej na nośniku startowym i odzyskiwanie jej (**entire_pc_cloud**)

- Tworzenie kopii zapasowej w udziale sieciowym i odzyskiwanie jej (**entire_pc_cloud**)
- Odzyskiwanie z magazynu w chmurze (**golden_image**)

Skrypty można znaleźć w następujących katalogach na komputerze z zainstalowanym generatorem nośnika startowego:

- W systemie Windows: %**ProgramData%\Acronis\MediaBuilder\scripts**
- W systemie Linux: **/var/lib/Acronis/MediaBuilder/scripts/**

Tworzenie kopii zapasowej w magazynie w chmurze i odzyskiwanie jej

Ten skrypt utworzy kopię zapasową komputera w magazynie w chmurze lub odzyska dane komputera z najbardziej aktualnej kopii zapasowej utworzonej w magazynie w chmurze za pomocą tego skryptu. Po uruchomieniu skrypt wyświetli monit o wybranie kopii zapasowej, odzyskiwania lub uruchomienia interfejsu użytkownika.

W generatorze nośnika startowego określ następujące parametry skryptu:

1. Nazwa użytkownika i hasło dla magazynu w chmurze.
2. [Opcjonalnie] Hasło, którego skrypt będzie używać do szyfrowania lub uzyskiwania dostępu do kopii zapasowych.

Tworzenie kopii zapasowej na nośniku startowym i odzyskiwanie jej

Ten skrypt utworzy kopię zapasową komputera na nośniku startowym lub odzyska dane komputera z najbardziej aktualnej kopii zapasowej utworzonej za pomocą tego skryptu na tym samym nośniku. Po uruchomieniu skrypt wyświetli monit o wybranie kopii zapasowej, odzyskiwania lub uruchomienia interfejsu użytkownika.

W generatorze nośnika startowego możesz określić hasło, którego skrypt będzie używać do szyfrowania lub uzyskiwania dostępu do kopii zapasowych.

Tworzenie kopii zapasowej w udziale sieciowym i odzyskiwanie jej

Ten skrypt utworzy kopię zapasową komputera w udziale sieciowym lub odzyska dane komputera z najbardziej aktualnej kopii zapasowej znajdującej się w udziale sieciowym. Po uruchomieniu skrypt wyświetli monit o wybranie kopii zapasowej, odzyskiwania lub uruchomienia interfejsu użytkownika.

W generatorze nośnika startowego określ następujące parametry skryptu:

1. Ścieżka udziału sieciowego.
2. Nazwa użytkownika i hasło dla udziału sieciowego.
3. [Opcjonalnie] Nazwa pliku kopii zapasowej. Wartość domyślna to **AutoBackup**. Jeśli chcesz, aby skrypt dołączał kopie zapasowe do istniejącej kopii zapasowej lub odzyskiwał dane z kopii zapasowej o nazwie innej niż domyślna, zmień wartość domyślną na nazwę pliku tej kopii zapasowej.

   Aby znaleźć nazwę pliku kopii zapasowej

a. W konsoli internetowej Cyber Protect przejdź do sekcji **Magazyn kopii zapasowych** > **Lokalizacje**.
b. Wybierz udział sieciowy (kliknij opcję **Dodaj lokalizację**, jeśli udziału nie ma na liście).
c. Wybierz kopię zapasową.
d. Kliknij opcję **Szczegóły**. Nazwa pliku jest wyświetlana w pozycji **Nazwa pliku kopii zapasowej**.

4. [Opcjonalnie] Hasło, którego skrypt będzie używać do szyfrowania lub uzyskiwania dostępu do kopii zapasowych.

Odzyskiwanie z magazynu w chmurze

Ten skrypt odzyska dane komputera z najbardziej aktualnej kopii zapasowej znajdującej się w magazynie w chmurze. Po uruchomieniu skrypt wyświetli monit o określenie następujących elementów:

1. Nazwa użytkownika i hasło dla magazynu w chmurze.
2. Hasło, jeśli kopia zapasowa jest szyfrowana.

W ramach tego konta magazynu w chmurze zalecamy przechowywanie kopii zapasowych tylko jednego komputera. W przeciwnym wypadku, jeśli kopia zapasowa innego komputera będzie nowsza niż kopia zapasowa bieżącego komputera, skrypt wybierze tę kopię zapasową komputera.

Skrypty niestandardowe

Ważne
Tworzenie skryptów niestandardowych wymaga znajomości języka poleceń Bash i notacji obiektu JavaScript (JSON). Jeśli nie znasz języka Bash, dobrym miejscem, aby się go nauczyć, jest http://www.tldp.org/LDP/abs/html. Specyfikacja notacji JSON jest dostępna pod adresem http://www.json.org

Pliki skryptu

Skrypt musi się znajdować w następujących katalogach na komputerze z zainstalowanym generatorem nośnika startowego:

- W systemie Windows: %**ProgramData%\Acronis\MediaBuilder\scripts**
- W systemie Linux: **/var/lib/Acronis/MediaBuilder/scripts/**

Skrypt musi zawierać przynajmniej trzy pliki:

- **<script_file>.sh** — plik ze skryptem Bash. Podczas tworzenia skryptu używaj tylko ograniczonego zestawu poleceń powłoki, które możesz znaleźć pod adresem https://busybox.net/downloads/BusyBox.html. Ponadto można użyć następujących poleceń:
  - `acrocmd` — narzędzie wiersza polecenia do tworzenia kopii zapasowych i odzyskiwania
  - `product` — polecenie uruchamiające interfejs użytkownika nośnika startowego

Ten i wszelkie dodatkowe pliki uwzględnione w skrypcie (na przykład za pomocą polecenia dot) muszą się znajdować w podfolderze **bin**. W skrypcie określ ścieżki dodatkowych plików w następującej postaci: **/ConfigurationFiles/bin/<plik>**.

- **autostart** — plik do uruchamiania pliku **<plik_skryptu>.sh**. Zawartość pliku musi być następująca:

```
#!/bin/sh
. /ConfigurationFiles/bin/variables.sh
. /ConfigurationFiles/bin/<script_file>.sh
. /ConfigurationFiles/bin/post_actions.sh
```

- **autostart.json** — plik JSON zawierający poniższe:
  - Nazwa i opis skryptu wyświetlane w generatorze nośnika startowego.
  - Nazwy zmiennych skryptu, które mają zostać skonfigurowane za pomocą generatora nośnika startowego.
  - Parametry elementów sterujących wyświetlane w generatorze nośnika startowego dla każdej zmiennej.

Struktura pliku autostart.json

Obiekt najwyższego poziomu

Para		Wymagane	Opis
Nazwa	**Typ wartości**		
`displayName`	ciąg	Tak	Nazwa skryptu wyświetlana w generatorze nośnika startowego.
`description`	ciąg	Nie	Opis skryptu wyświetlany w generatorze nośnika startowego.
`timeout`	liczba	Nie	Limit czasu (w sekundach) dla menu startowego przed uruchomieniem skryptu. Jeśli para nie jest określona, limit czasu będzie wynosił 10 sekund.
`variables`	obiekt	Nie	Wszelkie zmienne dla pliku **<plik_skryptu>.sh**, które chcesz skonfigurować za pomocą generatora nośnika startowego. Wartość powinna być zestawem następujących par: identyfikator ciągu zmiennej i obiekt zmiennej (patrz tabela poniżej).

Obiekt zmiennej

Para		Wymagane	Opis
Nazwa	**Typ wartości**		
`displayName`	ciąg	Tak	Nazwa zmiennej używana w pliku **<plik_skryptu>.sh**.
`type`	ciąg	Tak	Typ elementu sterującego wyświetlanego w generatorze nośnika startowego. Ten element sterujący służy do konfiguracji wartości zmiennej. Wszystkie obsługiwane typy znajdują się w poniższej tabeli.
`description`	ciąg	Tak	Etykieta elementu sterującego wyświetlana nad elementem sterującym w generatorze nośnika startowego.
`default`	ciąg, jeśli `type` to `string`, `multiString`, `password` lub `enum` liczba, jeśli `type` to `number`, `spinner` lub `checkbox`	Nie	Wartość domyślna elementu sterującego. Jeśli para nie jest określona, wartością domyślną będzie ciąg pusty lub zero w zależności od typu elementu sterującego. Wartością domyślną pola wyboru może być `0` (stan skasowany) lub `1` (stan wybrany).
`order`	liczba (nieujemna)	Tak	Kolejność elementów sterujących w generatorze nośnika startowego. Im wyższa wartość, tym niżej element sterujący jest umieszczany względem innych elementów sterujących w pliku **autostart.json**. Wartość początkowa musi być równa `0`.
`min` (tylko dla wartości `spinner`)	liczba	Nie	Minimalna wartość pokrętła w polu pokrętła. Jeśli para nie jest określona, wartość będzie równa `0`.
`max` (tylko dla wartości `spinner`)	liczba	Nie	Maksymalna wartość pokrętła w polu pokrętła. Jeśli para nie jest określona, wartość będzie równa `100`.

`step` (tylko dla wartości `spinner`)	liczba	Nie	Wartość kroku pokrętła w polu pokrętła. Jeśli para nie jest określona, wartość będzie równa `1`.
`items` (tylko dla wartości `enum`)	tablica ciągów	Tak	Wartości dla listy rozwijanej.
`required` (dla `string`, `multiString`, `password` i `enum`)	liczba	Nie	Określa, czy wartość elementu sterującego może być pusta (`0`), czy też nie (`1`). Jeśli para nie jest określona, wartość elementu sterującego może być pusta.

Typ elementu sterującego

Nazwa	Opis
`string`	Jednowierszowe, nieograniczone pole tekstowe służące do wprowadzania lub edytowania krótkich ciągów.
`multiString`	Wielowierszowe, nieograniczone pole tekstowe służące do wprowadzania lub edytowania długich ciągów.
`password`	Jednowierszowe, nieograniczone pole tekstowe służące do bezpiecznego wprowadzania haseł.
`number`	Jednowierszowe, tylko numeryczne pole tekstowe służące do wprowadzania lub edytowania liczb.
`spinner`	Jednowierszowe, tylko numeryczne pole tekstowe służące do wprowadzania lub edytowania liczb z pokrętłem. Nazywane też polem pokrętła.
`enum`	Standardowa lista rozwijana ze stałym zestawem wstępnie określonych wartości.
`checkbox`	Pole wyboru z dwoma stanami — stanem skasowanym lub stanem wybranym.

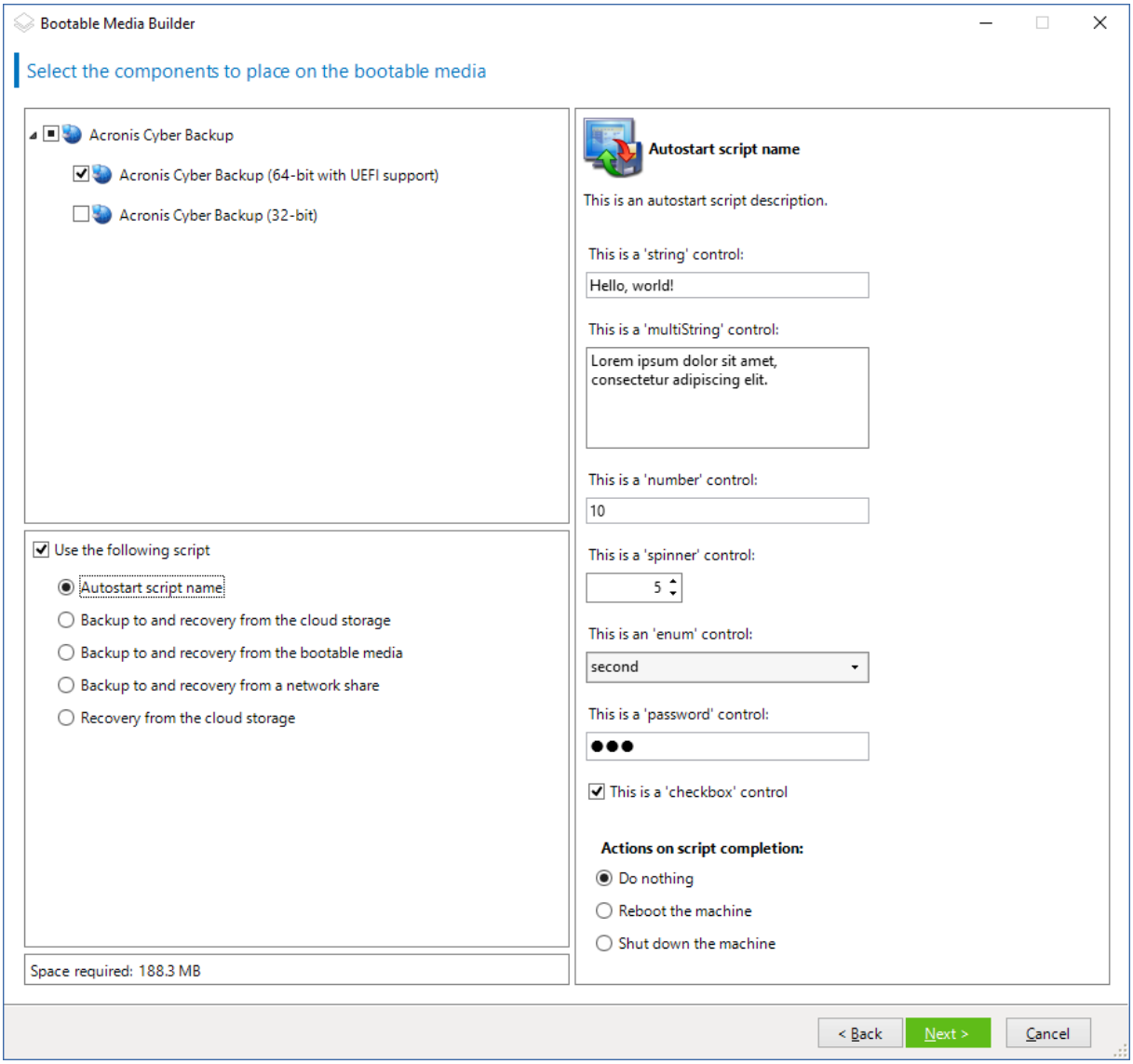
Przykładowy plik **autostart.json** poniżej zawiera wszystkie możliwe typy elementów sterujących, których można używać do konfiguracji zmiennych dla pliku **<script_file>.sh**.

```
{
        "displayName": "Autostart script name",
        "description": "This is an autostart script description.",
        "variables": {
                "var_string": {
```

```
                "displayName": "VAR_STRING",
                "type": "string", "order": 1,
                "description": "This is a 'string' control:", "default": "Hello,
world!"
        },
        "var_multistring": {
                "displayName": "VAR_MULTISTRING",
                "type": "multiString", "order": 2,
                "description": "This is a 'multiString' control:",
                "default": "Lorem ipsum dolor sit amet,\nconsectetur adipiscing elit."
        },
        "var_number": {
                "displayName": "VAR_NUMBER",
                "type": "number", "order": 3,
                "description": "This is a 'number' control:", "default": 10
        },
        "var_spinner": {
                "displayName": "VAR_SPINNER",
                "type": "spinner", "order": 4,
                "description": "This is a 'spinner' control:",
                "min": 1, "max": 10, "step": 1, "default": 5
        },
        "var_enum": {
                "displayName": "VAR_ENUM",
                "type": "enum", "order": 5,
                "description": "This is an 'enum' control:",
                "items": ["first", "second", "third"], "default": "second"
        },
        "var_password": {
                "displayName": "VAR_PASSWORD",
                "type": "password", "order": 6,
```

```
                "description": "This is a 'password' control:", "default": "qwe"
        },
        "var_checkbox": {
                "displayName": "VAR_CHECKBOX",
                "type": "checkbox", "order": 7,
                "description": "This is a 'checkbox' control", "default": 1
        }
    }
}
```

Tak to wygląda w generatorze nośnika startowego.



Serwer zarządzania

Podczas tworzenia nośnika startowego możesz wstępnie skonfigurować rejestrację nośnika na serwerze zarządzania.

Zarejestrowanie nośnika umożliwia zarządzanie nim przy użyciu konsoli internetowej Cyber Protect tak, jakby był zarejestrowanym komputerem. Poza wygodą związaną z dostępem zdalnym zapewnia to administratorowi możliwość śledzenia wszystkich operacji wykonywanych w ramach nośnika startowego. Operacje są rejestrowane w sekcji **Działania**, dzięki czemu można zobaczyć, kto rozpoczął operację i kiedy to zrobił.

Jeśli rejestracja nie została wstępnie skonfigurowana, nadal można zarejestrować nośnik po uruchomieniu komputera z nośnika.

Aby wstępnie skonfigurować rejestrację na serwerze zarządzania:

1. Zaznacz pole wyboru **Zarejestruj nośnik na serwerze zarządzania**.
2. W sekcji **Nazwa lub adres IP serwera** określ nazwę hosta lub adres IP komputera, na którym jest zainstalowany serwer zarządzania. Użyj jednego z następujących formatów:
   - `http://<serwer>`. Przykładowo `http://10.250.10.10` lub `http://serwer1`
   - `<adres IP>`. Na przykład `10.250.10.10`
   - `<nazwa hosta>`. Przykładowo `serwer1` lub `serwer1.przyklad.com`
3. W sekcji **Port** określ port, który będzie używany w celu uzyskania dostępu do serwera zarządzania. Wartość domyślna to 9877.
4. W polu **Nazwa wyświetlana** określ nazwę tego komputera, która ma być wyświetlana w konsoli internetowej Cyber Protect. Jeśli to pole pozostanie puste, nazwa wyświetlana zostanie ustawiona na jedną z poniższych:
   - Jeśli komputer był wcześniej zarejestrowany na serwerze zarządzania, będzie mieć tę samą nazwę.
   - W przeciwnym razie zostanie użyta w pełni kwalifikowana nazwa domeny (FQDN) lub adres IP komputera.
5. Wybierz konto, które będzie używane do rejestrowania nośnika na serwerze zarządzania. Dostępne są następujące opcje:
   - **Monituj o nazwę użytkownika i hasło podczas uruchamiania komputera**

     Podanie poświadczeń będzie wymagane za każdym razem, gdy komputer zostanie uruchomiony z nośnika.

     Aby zapewnić pomyślną rejestrację, konto musi się znajdować na liście administratorów serwera zarządzania (**Ustawienia** > **Konta**). W konsoli internetowej Cyber Protect nośnik będzie dostępny w ramach organizacji lub konkretnej jednostki, zgodnie z uprawnieniami danego konta.

     W interfejsie nośnika startowego można zmienić nazwę użytkownika i hasło, klikając kolejno **Narzędzia** > **Zarejestruj nośnik na serwerze zarządzania**.
   - **Zarejestruj przy użyciu niniejszego konta**

Komputer będzie rejestrowany automatycznie za każdym razem, gdy zostanie uruchomiony z nośnika.

Aby zapewnić pomyślną rejestrację, określone konto musi się znajdować na liście administratorów serwera zarządzania (**Ustawienia** > **Konta**). W konsoli internetowej Cyber Protect nośnik będzie dostępny w ramach organizacji lub konkretnej jednostki, zgodnie z uprawnieniami danego konta.

W interfejsie nośnika startowego *nie* można zmienić parametrów rejestracji.

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.

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 także 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.

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.

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 poddano migracji do innego sprzętu.

W narzędziu Universal Restore możliwe będzie skonfigurowanie:

- wyszukiwania na nośniku sterowników najlepiej dopasowanych do docelowego sprzętu,
- pobieranie z nośnika jawnie określonych sterowników pamięci masowej. Jest to konieczne, gdy docelowy komputer jest wyposażony w 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 docelowego komputera, 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**.

Nośnik startowy oparty na środowisku WinPE

Bootable Media Builder udostępnia dwie metody integracji programu Acronis Cyber Protect ze środowiskiem WinPE:

- Tworzenie od podstaw obrazu ISO środowiska PE z wtyczką.
- Dodanie wtyczki Acronis Plug-in do pliku WIM na potrzeby dowolnych przyszłych celów (ręcznego wygenerowania obrazu ISO, dodawania innych narzędzi do obrazu itd.).

Możesz tworzyć obrazy PE oparte na środowisku WinRE bez dodatkowych przygotowań lub tworzyć obrazy PE po zainstalowaniu Zestawu zautomatyzowanej instalacji systemu Windows (AIK) bądź Zestawu do oceny i wdrażania systemu Windows (ADK).

Obrazy PE oparte na środowisku WinRE

Tworzenie obrazów opartych na środowisku WinRE jest obsługiwane przez następujące systemy operacyjne:

- Windows 7 (64-bitowy)
- Windows 8, 8.1, 10 (32- i 64-bitowy)
- Windows Server 2012, 2016, 2019 (64-bitowy)

Obrazy PE

Po zainstalowaniu Zestawu zautomatyzowanej instalacji systemu Windows (AIK) bądź Zestawu do oceny i wdrażania systemu Windows (ADK) 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 z dodatkiem 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)

Program Bootable Media Builder 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.

Uwaga
Funkcja zarządzania dyskami jest niedostępna dla nośników startowych opartych na środowisku WinPE w wersji 4.0. Funkcja zarządzania dyskami jest dostępna dla systemu operacyjnego Windows 7 i wcześniejszych wersji. Aby wykonywać operacje zarządzania dyskami w systemie operacyjnym Windows 8 i nowszym, należy zainstalować program Acronis Disk Director. Więcej informacji można znaleźć w następującym artykule bazy wiedzy: https://kb.acronis.com/content/47031.

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=en
   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=en
   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=en
   Uzupełnienie zestawu zautomatyzowanej instalacji (AIK) dla systemu Windows 7 z dodatkiem SP1 (PE 3.1):
   http://www.microsoft.com/download/en/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.

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.

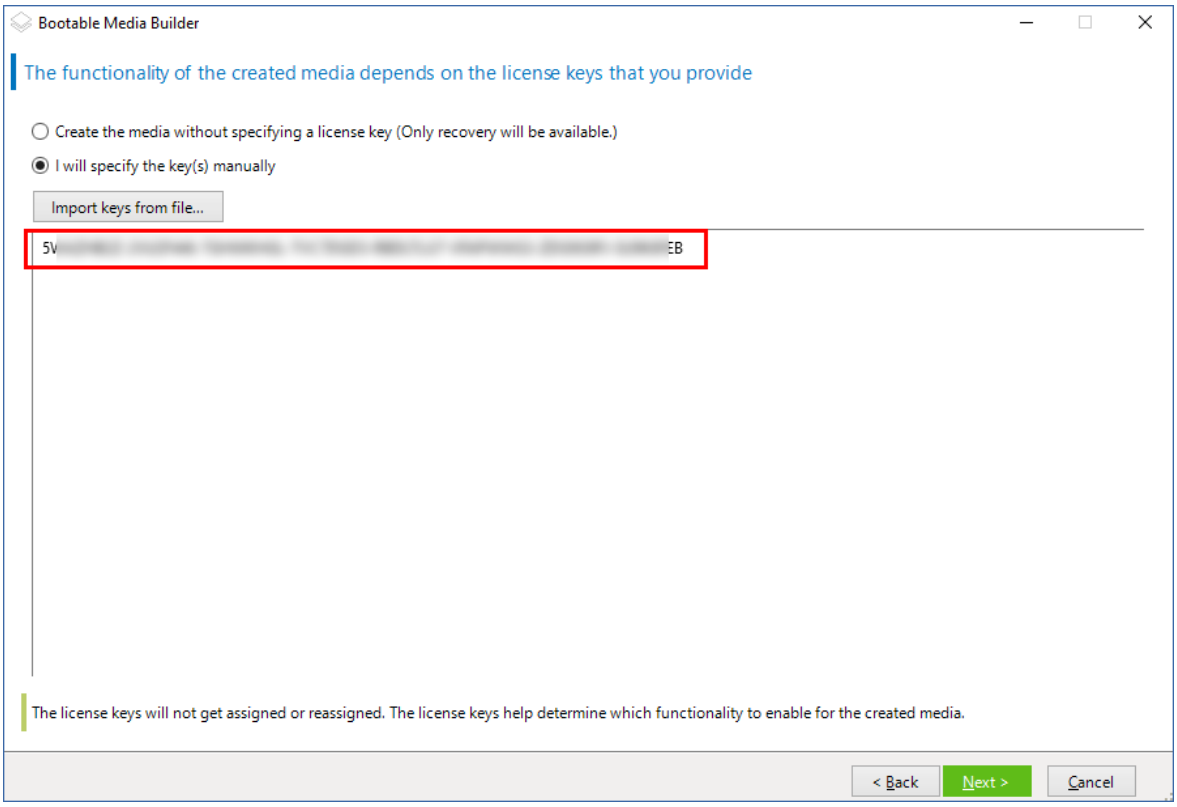
Aby przygotować komputer z zestawem ADK

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.
   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.

Dodawanie wtyczki Acronis Plug-in do środowiska WinPE

Aby dodać wtyczkę Acronis Plug-in do środowiska WinPE:

1. Uruchom Generator nośnika startowego.
2. Aby utworzyć w pełni funkcjonalny nośnik startowy, podaj klucz licencyjny programu Acronis Cyber Protect. Klucz ten posłuży do określenia, które funkcje zostaną uwzględnione na nośniku startowym. Żadna licencja nie zostanie odwołana z żadnego komputera.
   Jeśli nie podasz klucza licencyjnego, utworzonego nośnika startowego będzie można użyć tylko do operacji odzyskiwania.



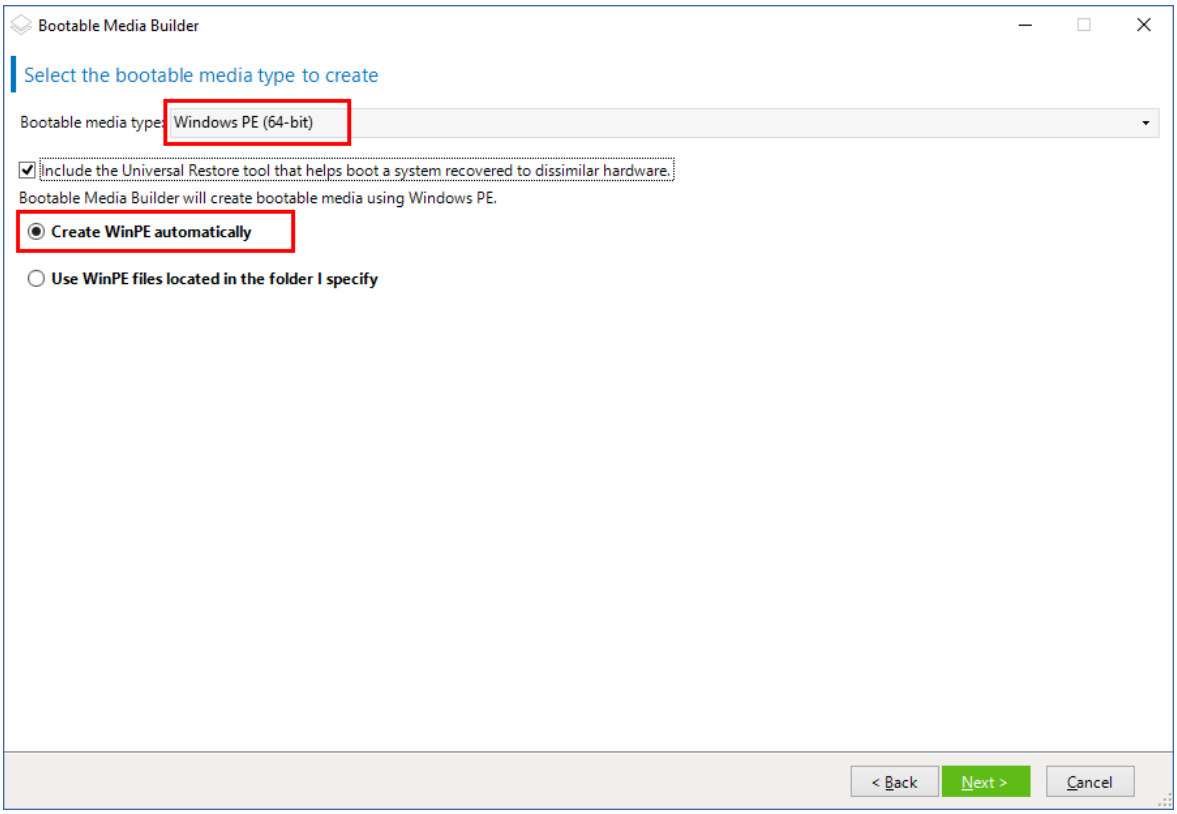
3. Wybierz **Typ nośnika startowego: Windows PE** lub **Typ nośnika startowego: Windows PE (64-bitowy)**. Nośnik 64-bitowy jest potrzebny do uruchomienia komputera korzystającego z interfejsu Unified Extensible Firmware Interface (UEFI).

   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**.

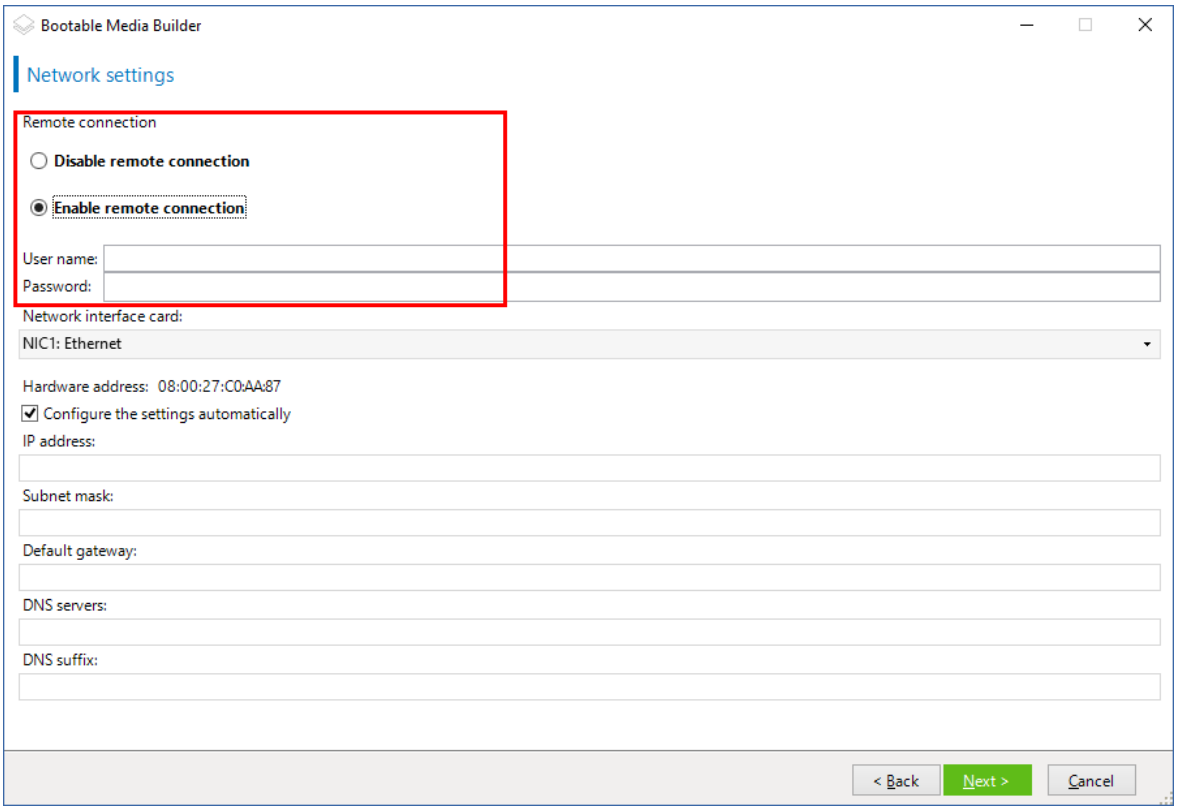
   Jeśli planujesz odzyskać system operacyjny na komputerze o innej konfiguracji sprzętowej lub na maszynie wirtualnej i chcesz zapewnić możliwość uruchamiania systemu, zaznacz pole wyboru **Uwzględnij narzędzie Universal Restore...**.
4. Wybierz **Utwórz WinPE automatycznie**.

   Oprogramowanie uruchamia odpowiedni skrypt i przechodzi do kolejnego okna.



5. Wybierz język, który będzie używany na nośniku startowym.
6. 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. Możesz też zostawić te pola puste, dzięki czemu zdalne połączenie przez interfejs wiersza polecenia będzie można nawiązać bez podawania poświadczeń.

   Te poświadczenia są też wymagane podczas rejestrowania nośnika na serwerze zarządzania z poziomu konsoli internetowej Cyber Protect.



7. Określ ustawienia sieciowe kart sieciowych komputera lub wybierz automatyczną konfigurację DHCP.

   Uwaga
   Ustawienia sieciowe są dostępne tylko w przypadku licencji Acronis Cyber Protect 15 Advanced i Acronis Cyber Protect 15 Backup Advanced. Szczegółowe porównanie funkcji można znaleźć w tym artykule w bazie Knowledge Base.

8. [Opcjonalnie] Podczas uruchamiania wybierz sposób rejestracji nośnika na serwerze zarządzania. Aby uzyskać więcej informacji na temat ustawień rejestrowania, zobacz Serwer zarządzania.
9. [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 komponentu 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 lub SATA, adaptera sieciowego, napędu taśmowego albo innego urządzenia.

- Powtórz tę procedurę w odniesieniu do każdego sterownika, który chcesz dołączyć do wynikowego nośnika środowiska WinPE.

10. Wybierz, czy chcesz utworzyć obraz ISO czy obraz WIM, lub prześlij nośnik na serwer (WDS lub RIS).
11. Określ pełną ścieżkę do wynikowego pliku obrazu, włącznie z nazwą pliku, lub określ serwer i podaj nazwę użytkownika oraz hasło umożliwiające do niego dostęp.
12. Na ekranie podsumowania sprawdź ustawienia i kliknij **Kontynuuj**.
13. Nagraj obraz ISO na płycie CD lub DVD za pomocą narzędzia innej firmy albo przygotuj startowy 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
```

Ostrzeżenie!
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.

Nawiązywanie połączenia z komputerem uruchomionym z nośnika

Po uruchomieniu komputera z nośnika startowego terminal komputera wyświetla okno uruchamiania z adresami IP uzyskanymi z serwera DHCP lub ustawionymi zgodnie ze wstępnie skonfigurowanymi wartościami.

Konfigurowanie ustawień sieciowych

Aby zmienić ustawienia sieciowe bieżącej sesji, w oknie startowym kliknij **Konfiguruj sieć**. Wyświetlone okno **Ustawienia sieciowe** umożliwia konfigurowanie ustawień sieciowych każdej karty sieciowej (NIC) komputera.

Zmiany wprowadzone w trakcie sesji zostaną utracone po ponownym uruchomieniu komputera.

Dodawanie sieci VLAN

W oknie **Ustawienia sieciowe** można dodawać wirtualne sieci lokalne (VLAN). Funkcja ta jest przydatna, jeśli wymagany jest dostęp do lokalizacji kopii zapasowych uwzględnionej w określonej sieci VLAN.

Sieci VLAN służą głównie do dzielenia sieci lokalnych na segmenty. Karta sieciowa (NIC) podłączona do portu *access* przełącznika ma zawsze dostęp do sieci VLAN określonej w konfiguracji portu. Karta sieciowa (NIC) podłączona do portu *trunk* przełącznika ma dostęp do sieci VLAN dozwolonych w konfiguracji portu tylko w przypadku, gdy sieci te zostały określone w ustawieniach sieciowych.

Aby umożliwić dostęp do sieci VLAN za pomocą portu trunk

1. Kliknij **Dodaj sieć VLAN**.
2. Wybierz kartę sieciową, która umożliwia dostęp do sieci lokalnej obejmującej wymaganą sieć VLAN.
3. Określ identyfikator sieci VLAN.

Po kliknięciu **OK** na liście kart sieciowych pojawi się nowa pozycja.

Jeśli konieczne jest usunięcie sieci VLAN, kliknij pozycję odpowiadającą żądanej sieci VLAN, a następnie kliknij **Usuń sieć VLAN**.

Połączenie lokalne

Aby działać bezpośrednio na komputerze uruchomionym za pomocą nośnika startowego, w oknie startowym kliknij **Zarządzaj tym komputerem lokalnie**.

Połączenie zdalne

Aby zdalnie podłączyć nośnik, zarejestruj go na serwerze zarządzania zgodnie z opisem w sekcji „Rejestrowanie nośnika na serwerze zarządzania”.

Rejestrowanie nośnika na serwerze zarządzania

Zarejestrowanie nośnika startowego umożliwia zarządzanie nim przy użyciu konsoli internetowej Cyber Protect tak, jakby był zarejestrowanym komputerem. Dotyczy to wszystkich nośników startowych niezależnie od metody startu (nośnik fizyczny, Startup Recovery Manager, serwer Acronis PXE Server, WDS lub RIS). Program nie pozwala jednak zarejestrować nośnika startowego utworzonego w systemie macOS.

Zarejestrowanie nośnika jest możliwe tylko w przypadku, gdy do serwera zarządzania dodano co najmniej jedną licencję programu Acronis Cyber Protect Advanced.

Nośnik można zarejestrować z poziomu jego interfejsu użytkownika.

Parametry rejestracji mogą zostać wstępnie skonfigurowane za pomocą opcji Serwer zarządzania Generatora nośnika startowego. W przypadku gotowej konfiguracji wszystkich parametrów

rejestracji nośnik będzie automatycznie wyświetlany w konsoli internetowej Cyber Protect. Jeśli wstępnie skonfigurowano niektóre parametry, niektóre kroki w poniższych procedurach mogą być niedostępne.

Rejestrowanie nośnika z poziomu interfejsu użytkownika nośnika

Nośnik można pobrać lub utworzyć za pomocą Generatora nośnika startowego.

Aby zarejestrować nośnik z poziomu interfejsu użytkownika nośnika

1. Uruchom komputer przy użyciu nośnika.
2. Wykonaj jedną z następujących czynności:
   - W oknie uruchamiania w obszarze **Serwer zarządzania** kliknij **Edytuj**.
   - W interfejsie nośnika startowego kliknij **Narzędzia** > **Zarejestruj nośnik na serwerze zarządzania**.
3. W polu **Zarejestruj na hoście** określ nazwę hosta lub adres IP komputera, na którym jest zainstalowany serwer zarządzania. Użyj jednego z następujących formatów:
   - `http://<serwer>`. Na przykład `http://10.250.10.10` lub `http://serwer`
   - `<adres IP>`. Na przykład `10.250.10.10`
   - `<nazwa hosta>`. Na przykład `serwer` lub `serwer.przyklad.com`
4. W polach **Nazwa użytkownika** i **Hasło** podaj poświadczenia konta znajdującego się na liście administratorów serwera zarządzania (**Ustawienia** > **Konta**). W konsoli internetowej Cyber Protect nośnik będzie dostępny w ramach organizacji lub konkretnej jednostki, zgodnie z uprawnieniami danego konta.
5. W polu **Nazwa wyświetlana** określ nazwę tego komputera, która ma być wyświetlana w konsoli internetowej Cyber Protect. Jeśli to pole pozostanie puste, nazwa wyświetlana zostanie ustawiona na jedną z poniższych:
   - Jeśli komputer był wcześniej zarejestrowany na serwerze zarządzania, będzie mieć tę samą nazwę.
   - W przeciwnym razie zostanie użyta w pełni kwalifikowana nazwa domeny (FQDN) lub adres IP komputera.
6. Kliknij **OK**.

Lokalne operacje wykonywane przy użyciu nośnika startowego

Operacje dotyczące nośnika startowego przypominają operacje tworzenia kopii zapasowych i odzyskiwania wykonywane w ramach działającego systemu operacyjnego. Różnice są następujące:

1. W przypadku nośnika startowego z takimi woluminami jak w systemie Windows wolumin ma taką samą literę dysku jak w systemie Windows. Woluminom, które nie mają liter dysku w systemie Windows (np. wolumin „Zastrzeżone przez system”), są przypisywane niezajęte litery w

kolejności zgodnej z ich kolejnością na dysku.

Jeśli nośnik startowy nie wykryje na komputerze systemu Windows lub wykryje więcej niż jeden system, do wszystkich woluminów (włącznie z woluminami bez liter dysku) litery są przypisywane w takiej kolejności, w jakiej te woluminy występują na dysku. Oznacza to, że litery woluminów mogą się różnić od liter w systemie Windows. Na przykład dysk D: na nośniku startowym może odpowiadać dyskowi E: w systemie Windows.

Uwaga
Rekomendujemy przypisywać woluminom unikatowe nazwy.

2. W przypadku nośnika startowego z takimi woluminami jak w systemie Linux dyski lokalne i woluminy są wyświetlane jako niezamontowane (sda1, sda2...).
3. Kopie zapasowe tworzone przy użyciu nośników startowych charakteryzują się uproszczonym nazewnictwem plików. Standardowe nazwy są im nadawane tylko wtedy, gdy są dodawane do istniejącego już archiwum ze standardowym nazewnictwem plików lub gdy lokalizacja docelowa nie obsługuje uproszczonych nazw.
4. W przypadku nośnika startowego z takimi woluminami jak w systemie Linux kopie zapasowe nie mogą być zapisywane w woluminie sformatowanym w systemie NTFS. W razie potrzeby można zmienić nośnik na taki z woluminami jak w systemie Windows. Aby przełączyć reprezentację woluminów na nośniku startowym, kliknij **Narzędzia** > **Zmień reprezentację woluminu**.
5. Zadań nie można planować. Jeśli trzeba powtórzyć operację, należy skonfigurować ją od początku.
6. Czas życia dziennika jest ograniczony do bieżącej sesji. Cały dziennik lub odfiltrowane wpisy dziennika można zapisać w pliku.
7. Skarbce centralne nie są wyświetlane w drzewie folderów w oknie **Archiwum**.

   Aby uzyskać dostęp do skarbca zarządzanego, w polu **Ścieżka** wpisz:

   bsp://adres_węzła/nazwa_skarbca/

   Aby uzyskać dostęp do niezarządzanego skarbca centralnego, wpisz pełną ścieżkę do folderu skarbca.

   Po wprowadzeniu poświadczeń dostępu zostanie wyświetlona lista archiwów znajdujących się w skarbcu.

Konfigurowanie trybu wyświetlania

W przypadku uruchamiania komputera przy użyciu nośnika startowego opartego na systemie Linux tryb wyświetlania obrazu wideo jest wykrywany automatycznie na podstawie konfiguracji sprzętowej (danych technicznych monitora i karty graficznej). Jeśli tryb wideo jest wykrywany niepoprawnie, wykonaj następujące czynności:

1. W menu startowym naciśnij F11.
2. Wpisz w wierszu polecenia: **vga=ask** i kontynuuj uruchamianie.
3. Z listy obsługiwanych trybów wideo wybierz odpowiedni tryb, wpisując jego numer (na przykład **318**), a następnie naciśnij klawisz **Enter**.

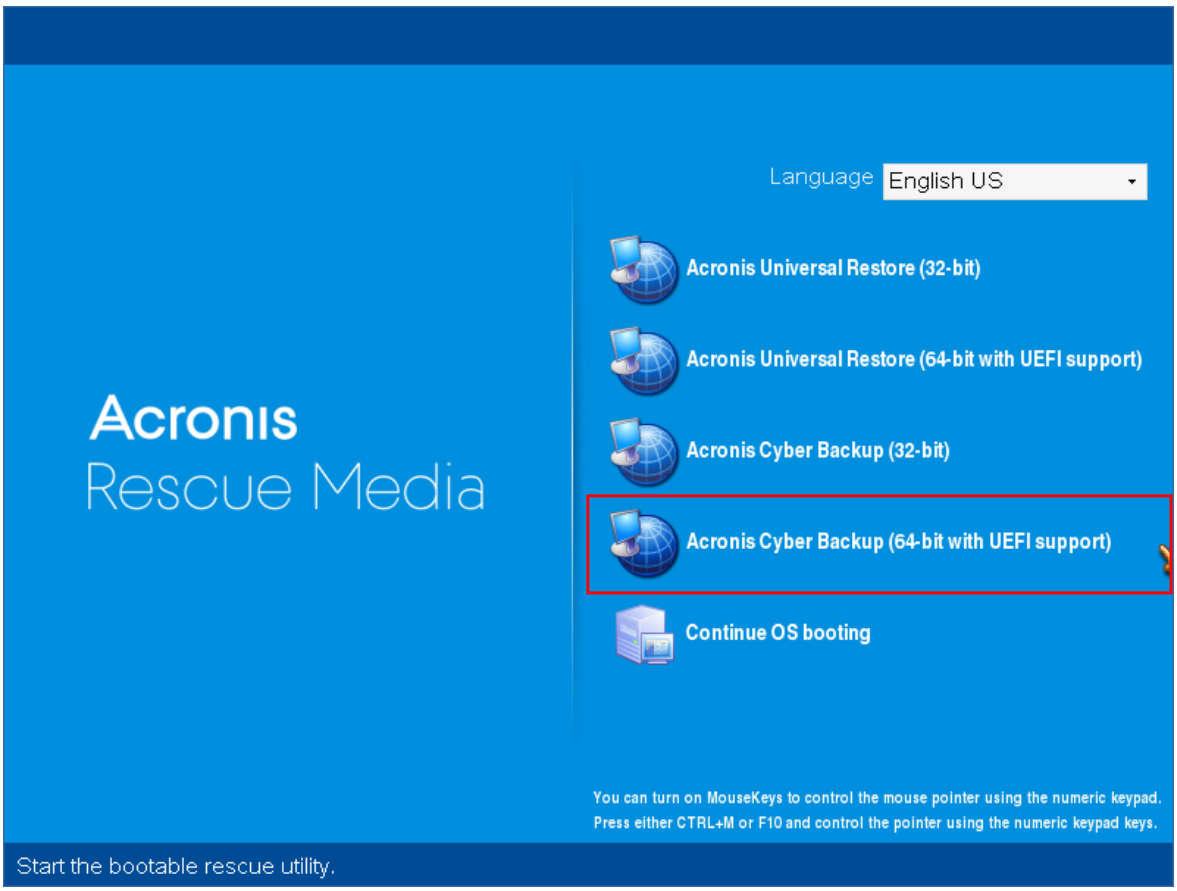
Jeśli nie chcesz wykonywać tej procedury przy każdym uruchamianiu danej konfiguracji sprzętowej, ponownie utwórz nośnik startowy, wprowadzając odpowiedni numer trybu (w tym przykładzie: **vga=0x318**) w oknie **Parametry jądra**.

Lokalne tworzenie kopii zapasowych przy użyciu nośnika startowego

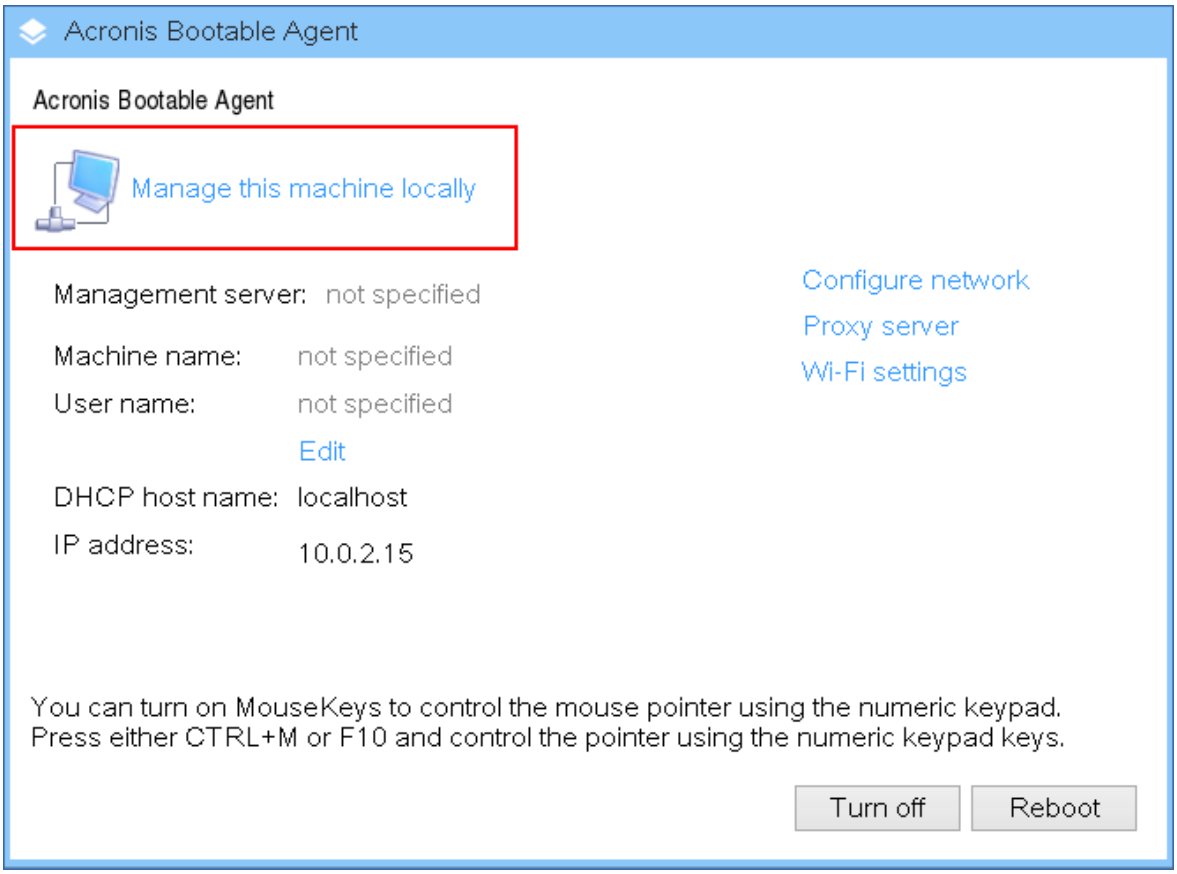
Możesz utworzyć kopię zapasową danych tylko przy użyciu nośnika startowego utworzonego za pomocą narzędzia Bootable Media Builder oraz przy użyciu klucza licencyjnego programu Acronis Cyber Protect. Więcej informacji na temat tworzenia nośnika startowego można znaleźć w sekcji Nośnik startowy oparty na systemie Linux lub Nośnik startowy oparty na środowisku Windows PE.

Aby utworzyć kopię zapasową danych przy użyciu nośnika startowego

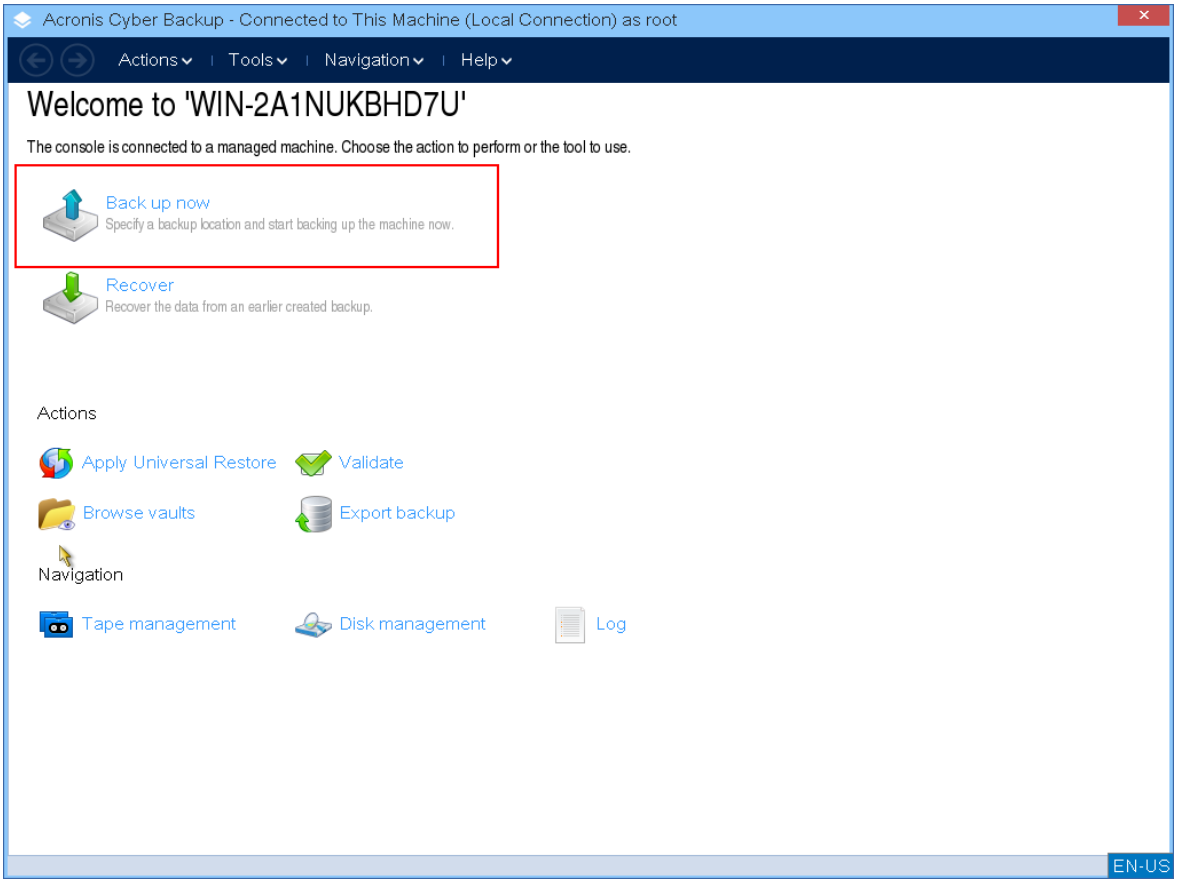
1. Uruchom z ratunkowego nośnika startowego firmy Acronis.



2. Aby utworzyć kopię zapasową komputera lokalnego, kliknij **Zarządzaj tym komputerem lokalnie**. W przypadku połączeń zdalnych zobacz sekcję Rejestrowanie nośnika na serwerze zarządzania.



3. Kliknij **Utwórz kopię zapasową**.

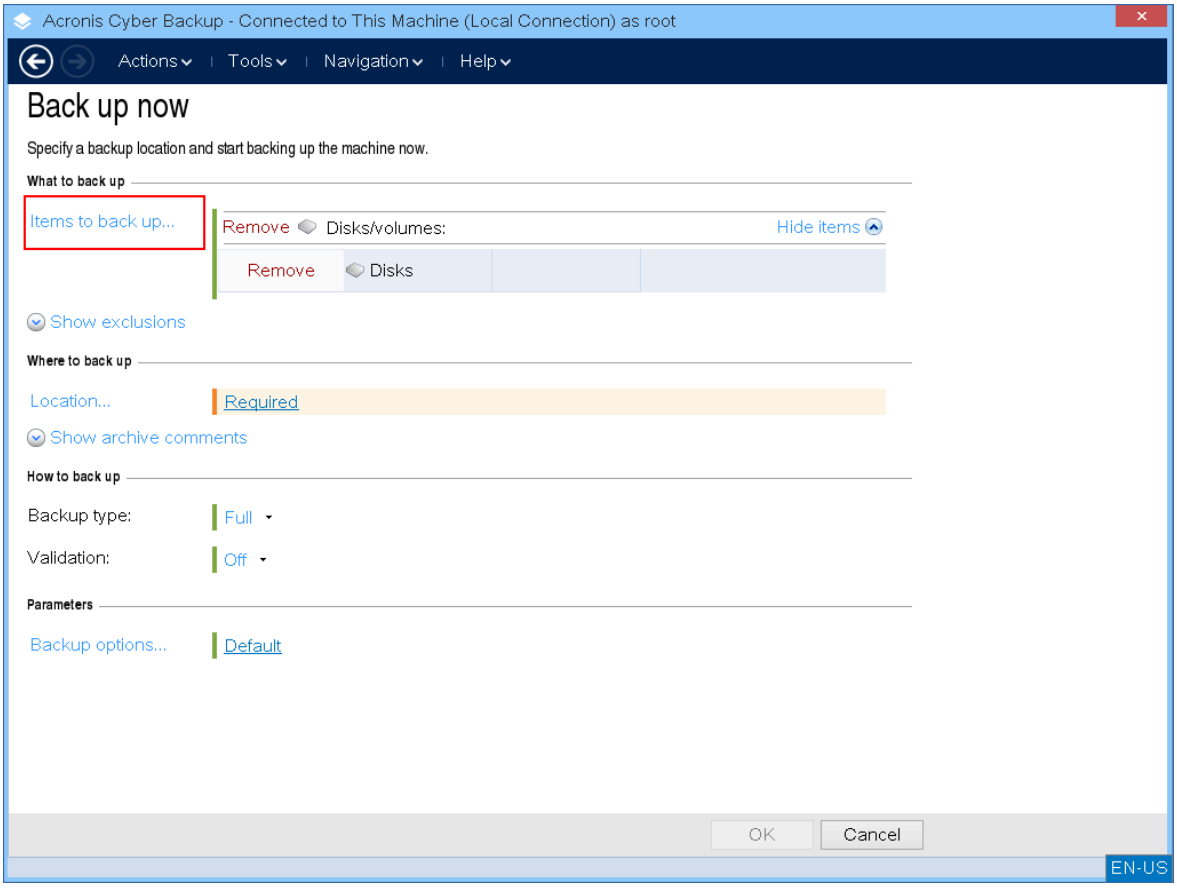


4. Do utworzenia kopii zapasowej automatycznie są wybierane wszystkie niewymienne dyski komputerów. Aby zmienić dane, które zostaną uwzględnione w kopii zapasowej, kliknij **Elementy uwzględniane w kopii zapasowej**, a następnie wybierz żądane dyski lub woluminy.

   Podczas wybierania danych do uwzględnienia w kopii zapasowej możesz zobaczyć następujący komunikat: *„Ten komputer nie może być wybrany bezpośrednio. Na komputerze jest zainstalowana poprzednia wersja agenta. W celu wybrania tego komputera do tworzenia kopii zapasowych skorzystaj z reguł zasad”.* Jest to problem związany z interfejsem graficznym, który spokojnie można zignorować. Następnie wybierz dyski lub woluminy, które chcesz uwzględnić w kopii zapasowej.

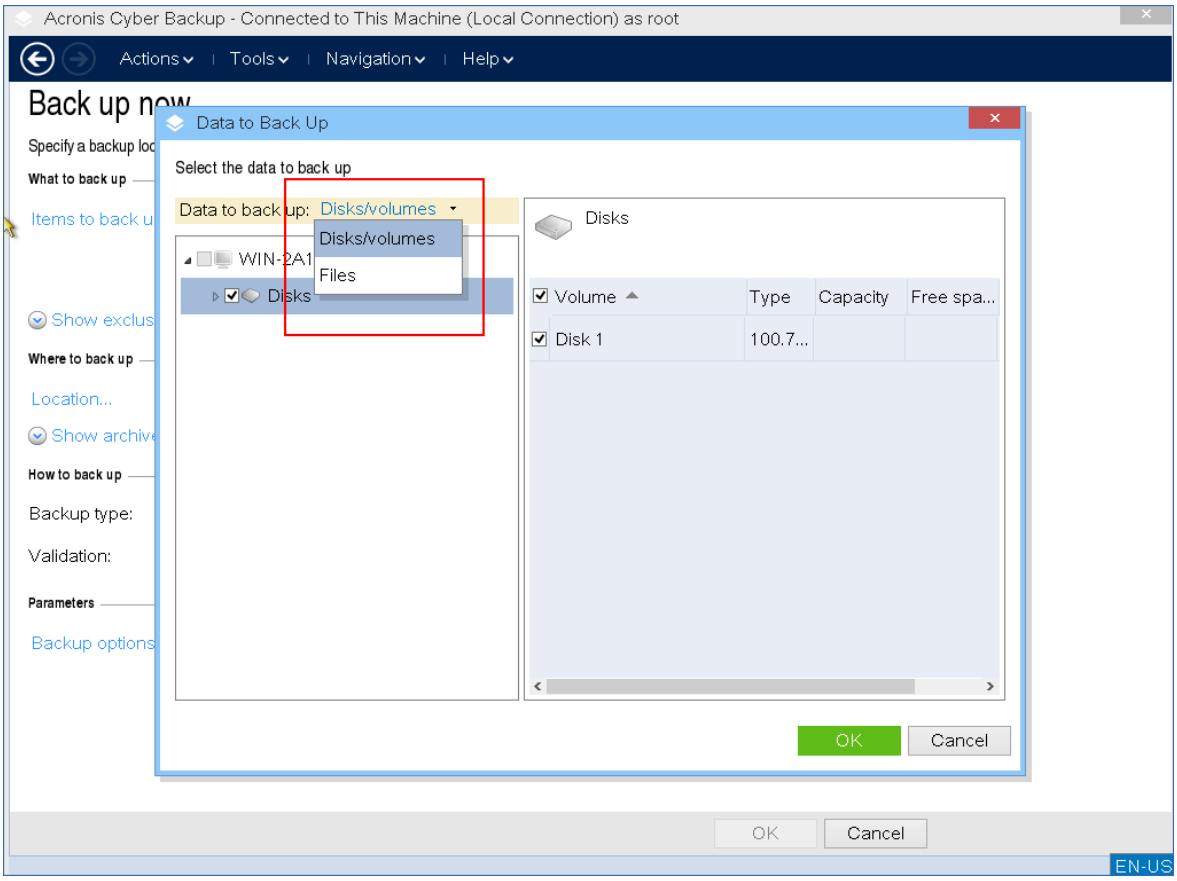
   Uwaga

   W przypadku nośnika startowego opartego na systemie Linux mogą się pojawić litery dysku inne niż te używane w systemie Windows. Spróbuj zidentyfikować potrzebny dysk lub partycję na podstawie rozmiaru lub etykiety.

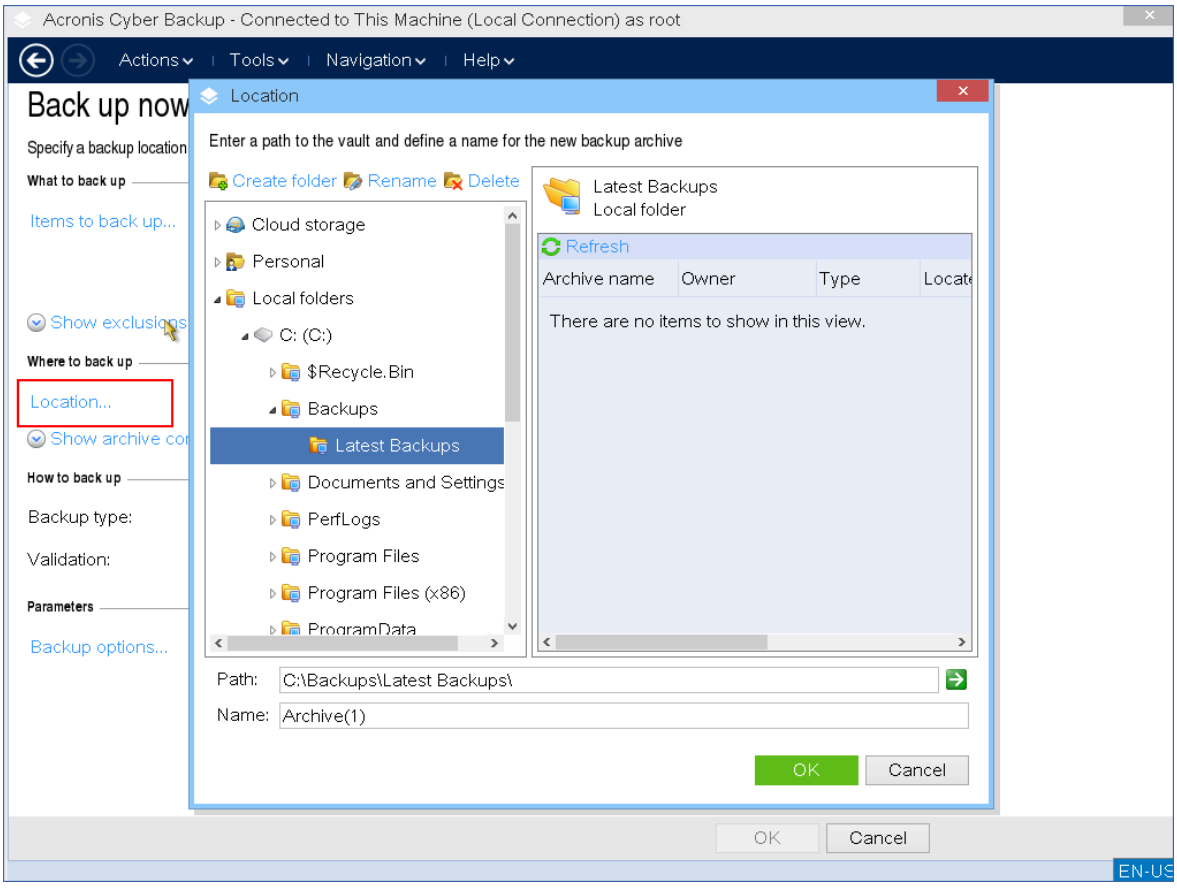


5. Jeśli chcesz utworzyć kopię zapasową plików lub folderów, a nie dysków, wybierz opcję **Pliki** w polu **Dane uwzględniane w kopii zapasowej**.

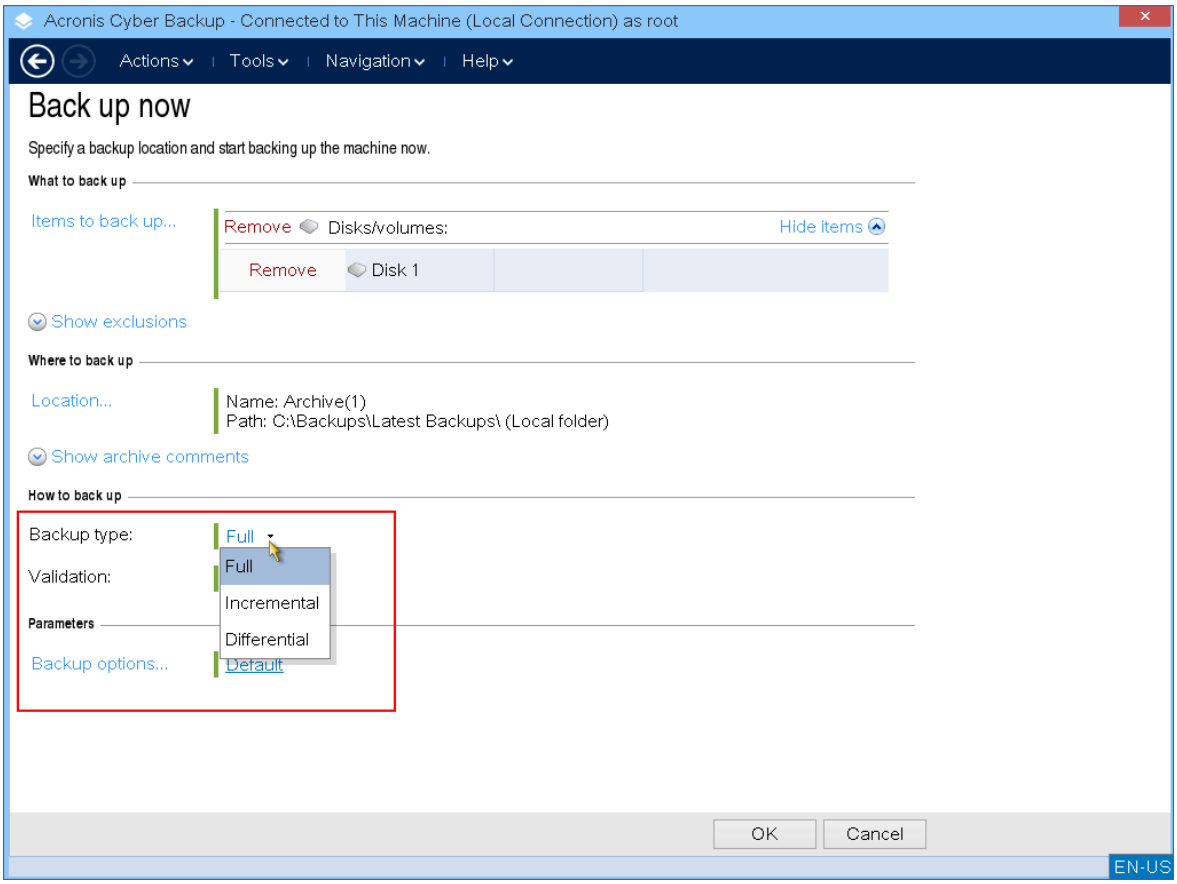
   W kontekście nośnika startowego dostępne są tylko kopie zapasowe dysków/partycji oraz plików/folderów. Inne typy kopii zapasowych, takie jak kopie zapasowe baz danych, są dostępne tylko w działającym systemie operacyjnym.



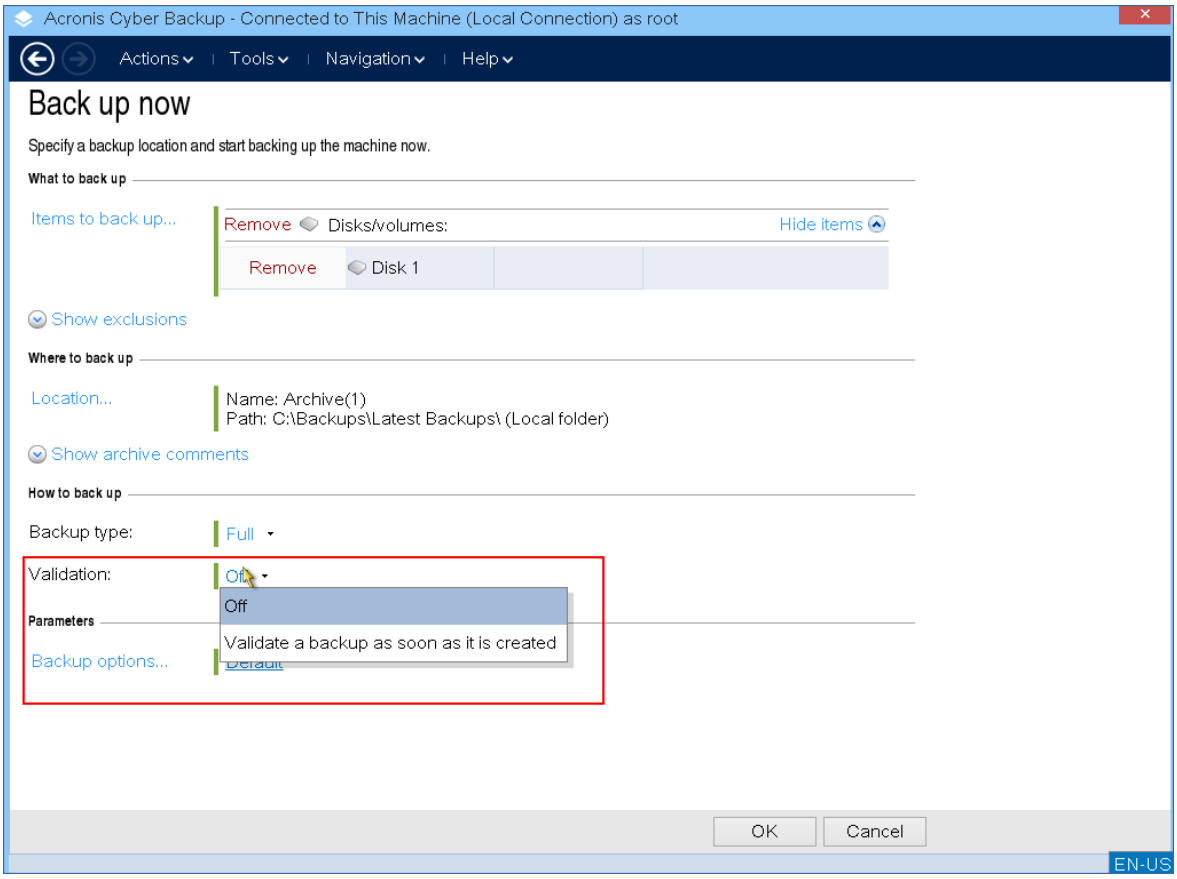
6. Kliknij **Lokalizacja**, aby wybrać miejsce zapisania kopii zapasowej.



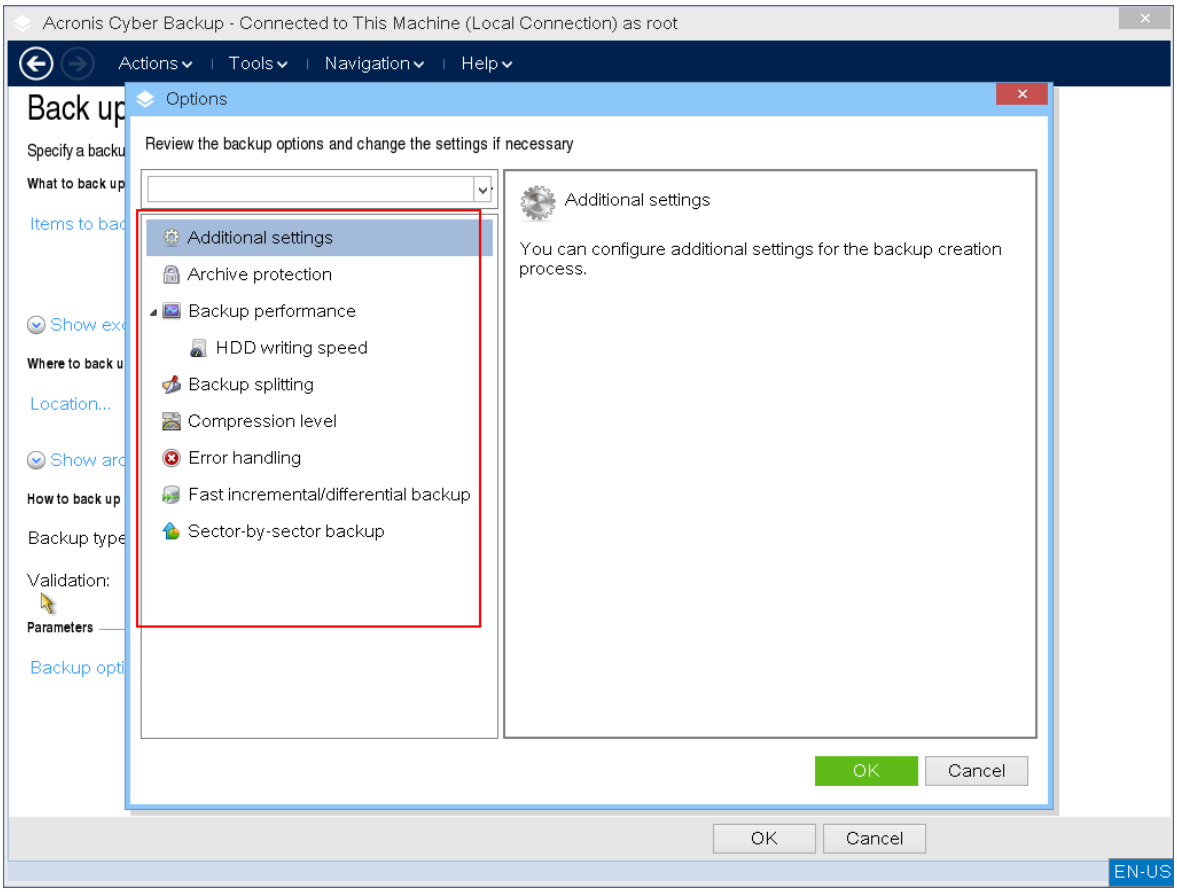
7. Określ lokalizację i nazwę kopii zapasowej.
8. Określ typ kopii zapasowej. Jeśli jest to pierwsza kopia zapasowa w tej lokalizacji, zostanie utworzona pełna kopia zapasowa. Jeśli kontynuujesz łańcuch kopii zapasowych, możesz wybrać opcję **Przyrostowa** lub **Różnicowa**, aby zaoszczędzić miejsce. Więcej informacji o typach kopii zapasowych można znaleźć na stronie https://kb.acronis.com/content/1536.



9. [Opcjonalnie] Jeśli chcesz sprawdzić poprawność pliku kopii zapasowej, wybierz **Sprawdzaj poprawność kopii zapasowej natychmiast po utworzeniu**.

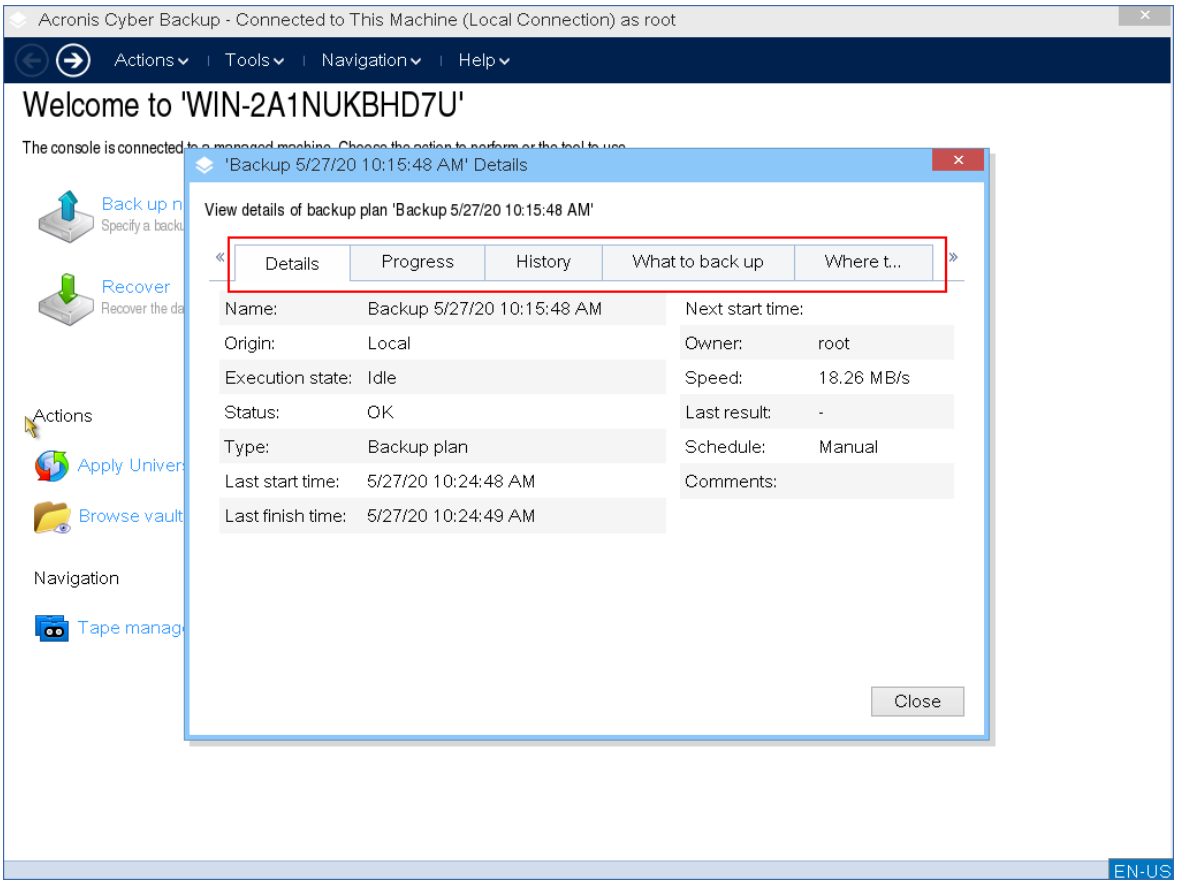


10. [Opcjonalnie] Określ opcje tworzenia kopii zapasowych, które mogą się przydać, np. hasło do pliku kopii zapasowej, podział kopii zapasowej lub obsługa błędów.



11. Kliknij **OK**, aby rozpocząć operację tworzenia kopii zapasowej.

    Nośnik startowy odczytuje dane z dysku, kompresuje je do pliku .tib, a następnie zapisuje ten plik w wybranej lokalizacji. Nie tworzy on migawki dysku, ponieważ nie są uruchomione żadne aplikacje.
12. W wyświetlonym oknie można sprawdzić status zadania tworzenia kopii zapasowej oraz dodatkowe informacje o kopii zapasowej.

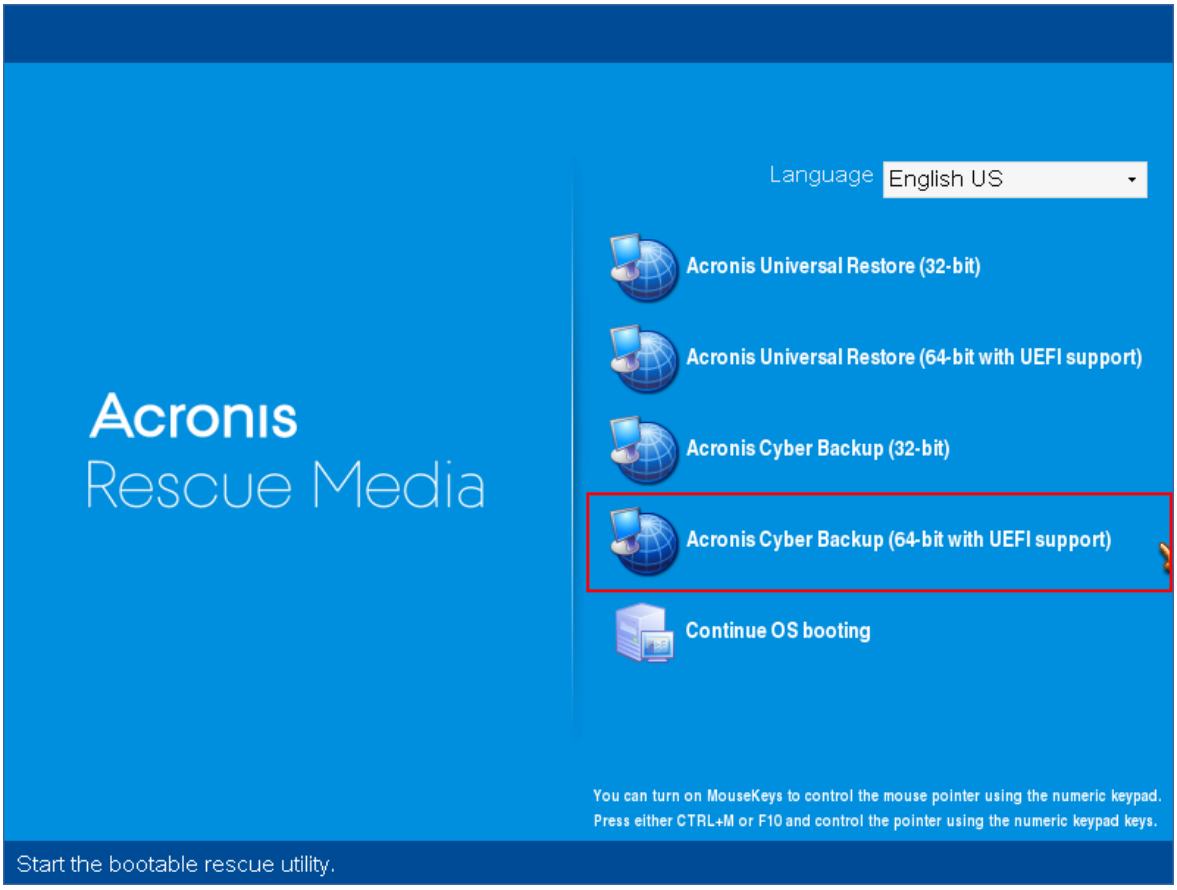


Odzyskiwanie lokalne przy użyciu nośnika startowego

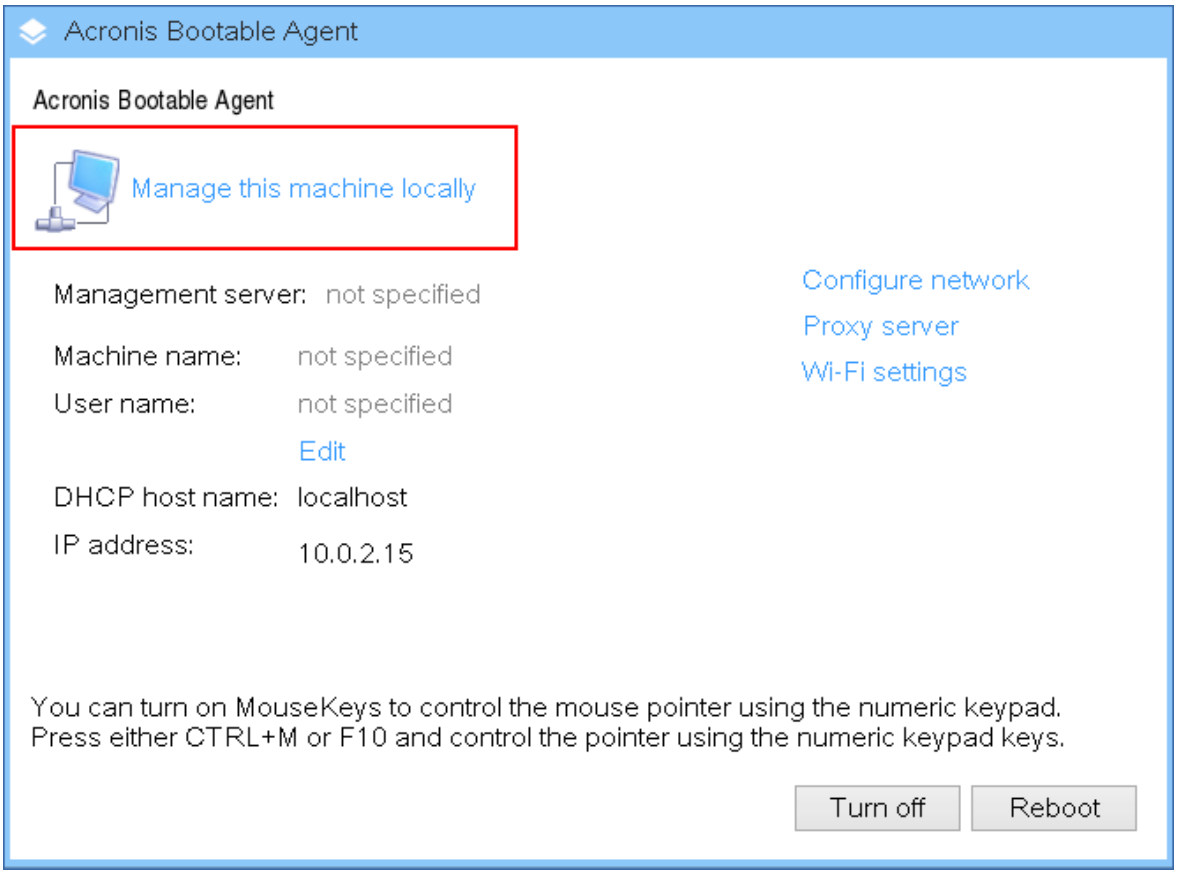
Operacja odzyskiwania jest dostępna zarówno w przypadku nośnika startowego utworzonego za pomocą Generatora nośnika startowego, jak i w przypadku pobranego gotowego nośnika startowego.

Aby odzyskać dane przy użyciu nośnika startowego

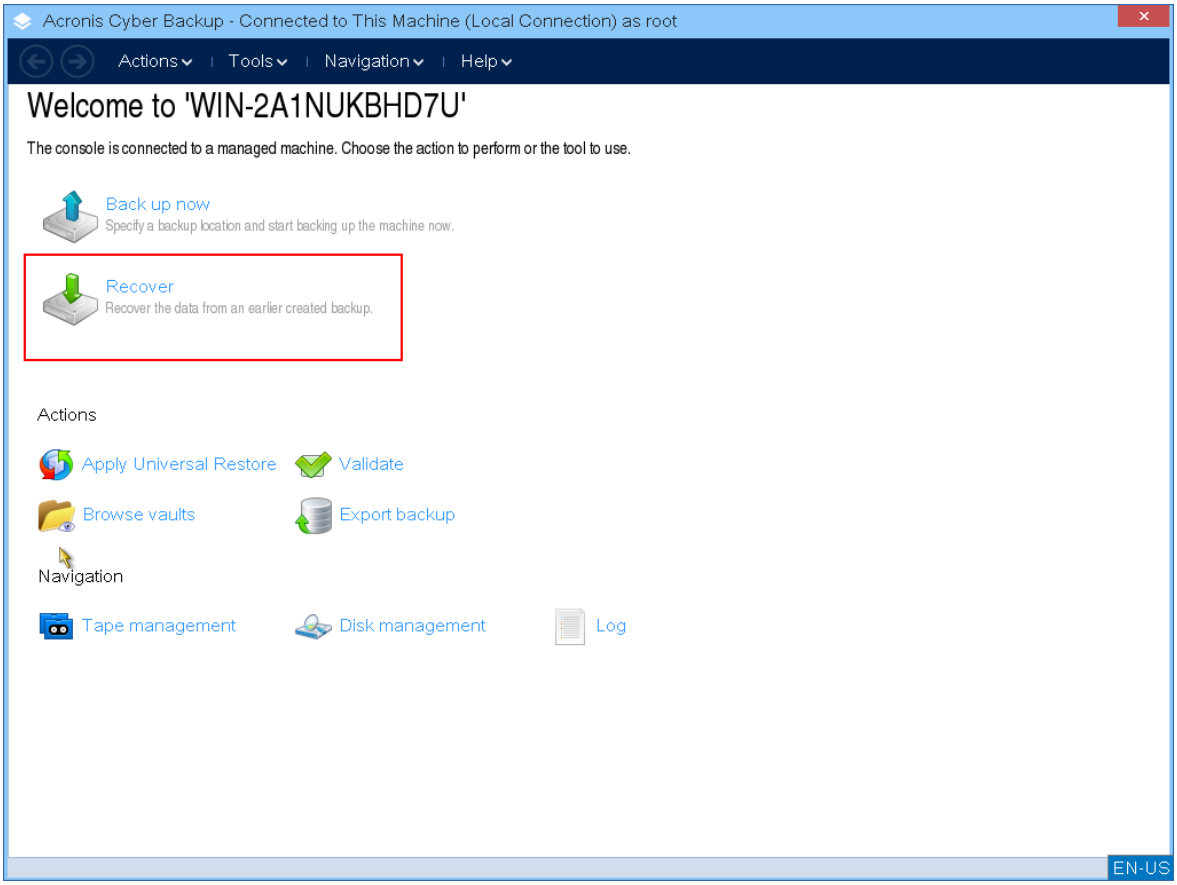
1. Uruchom z ratunkowego nośnika startowego firmy Acronis.



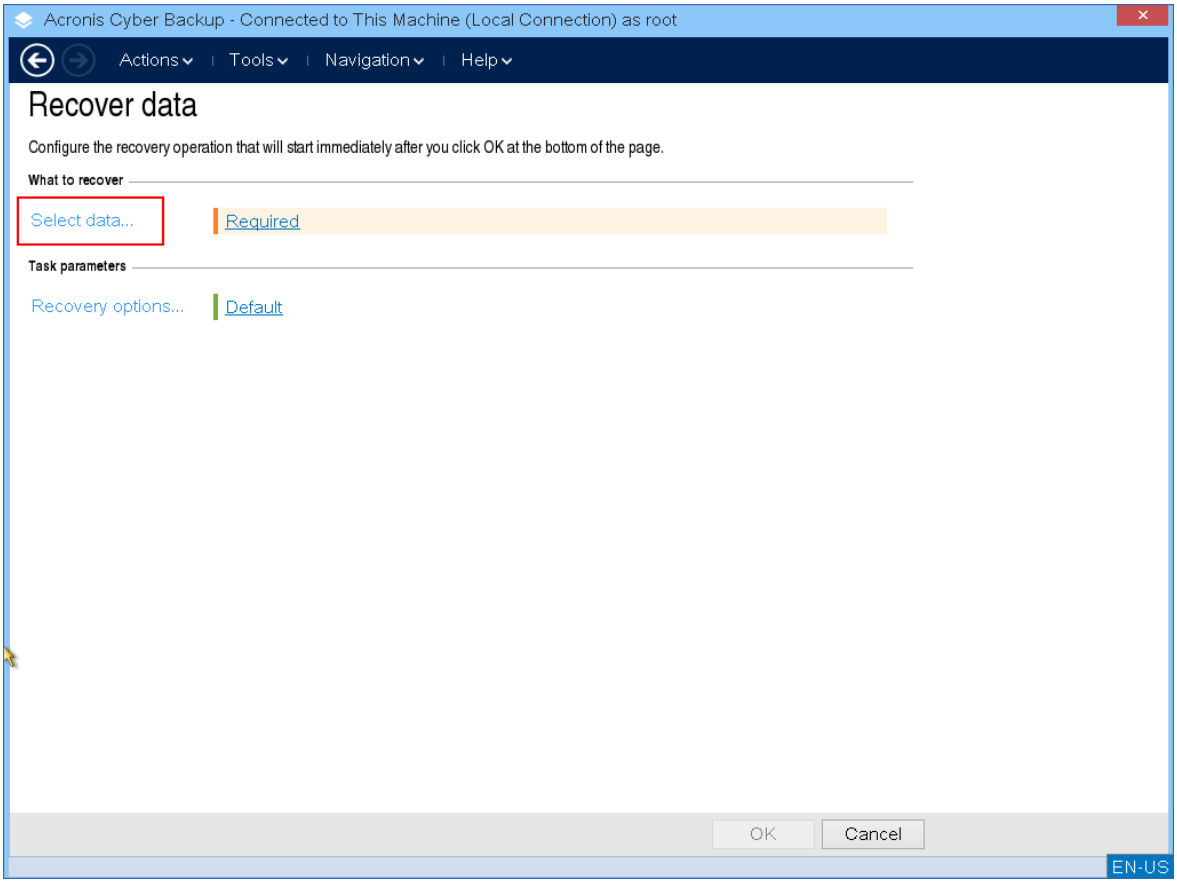
2. Aby odzyskać dane na komputer lokalny, kliknij **Zarządzaj tym komputerem lokalnie**. W przypadku połączeń zdalnych zobacz sekcję Rejestrowanie nośnika na serwerze zarządzania.



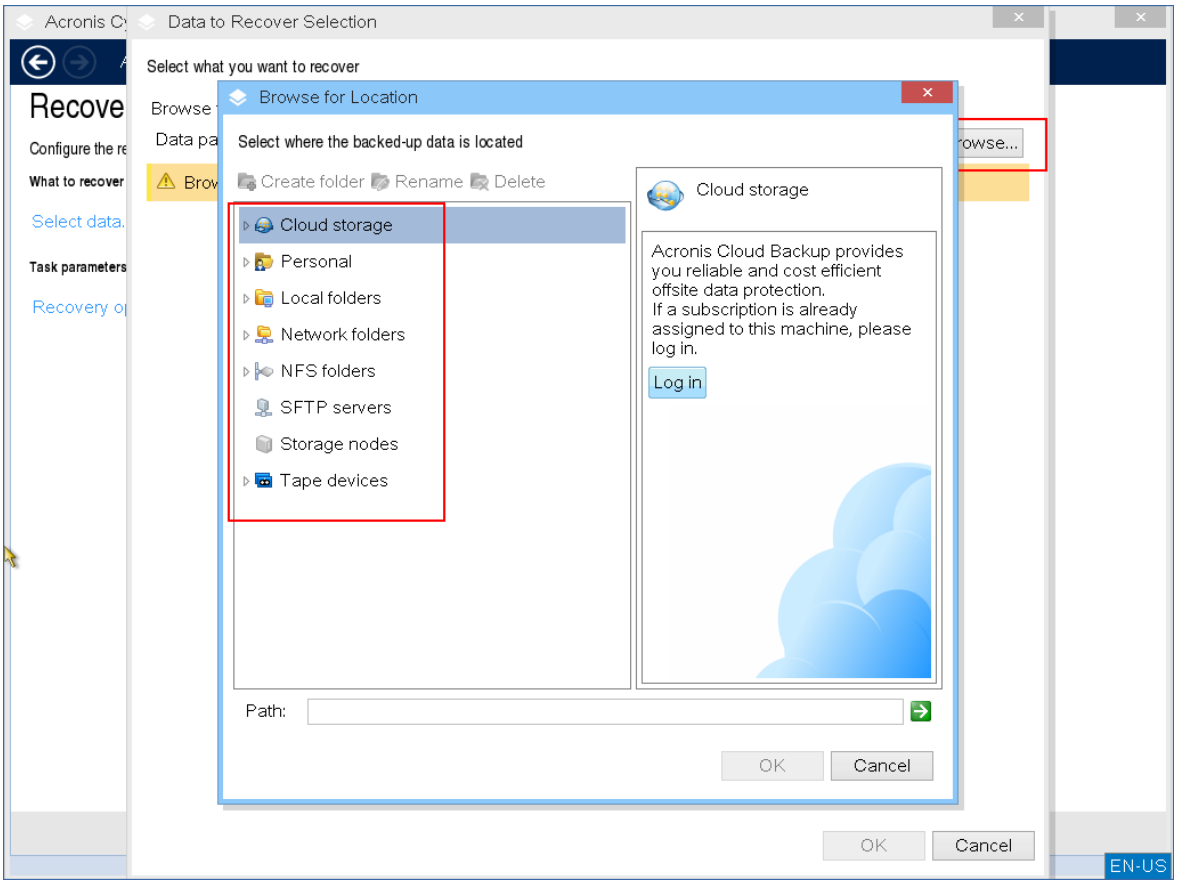
3. Kliknij **Odzyskaj**.



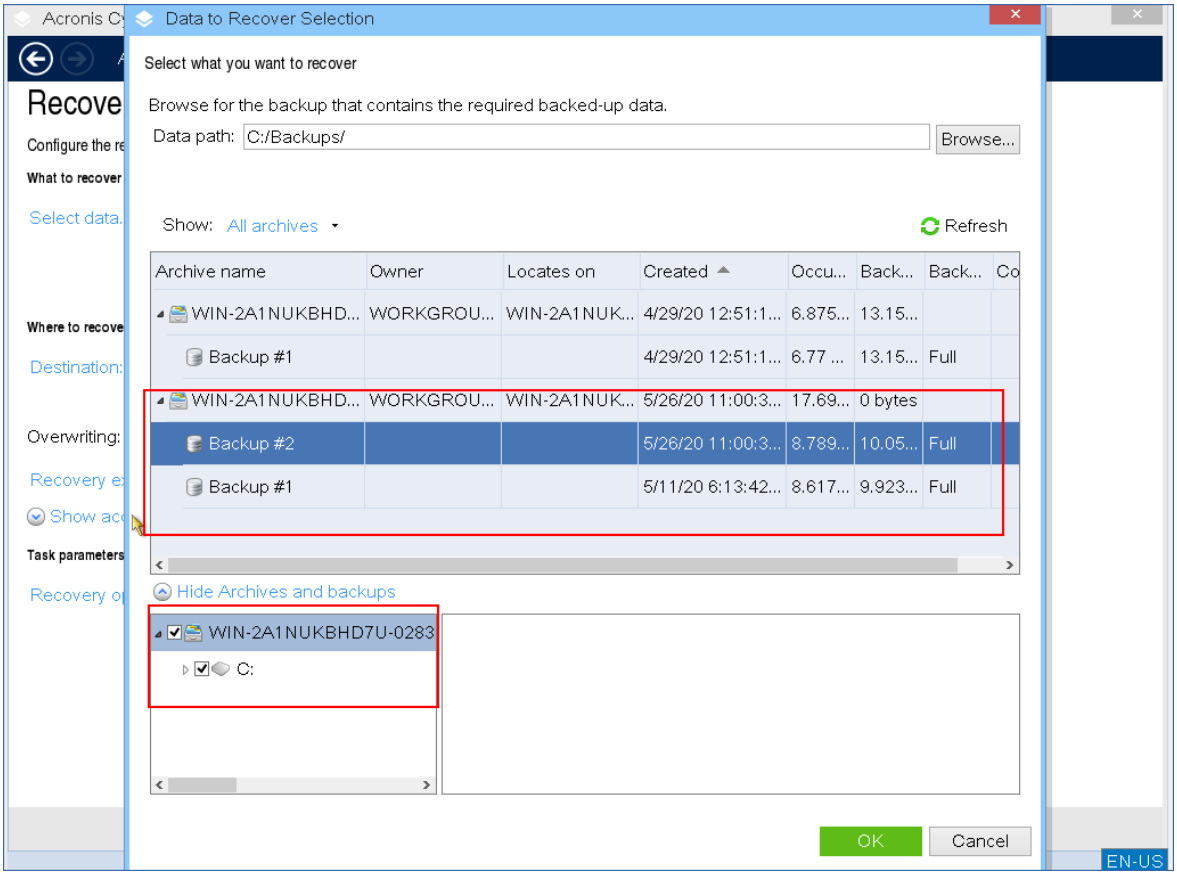
4. W sekcji **Elementy do odzyskania** kliknij **Wybierz dane**.



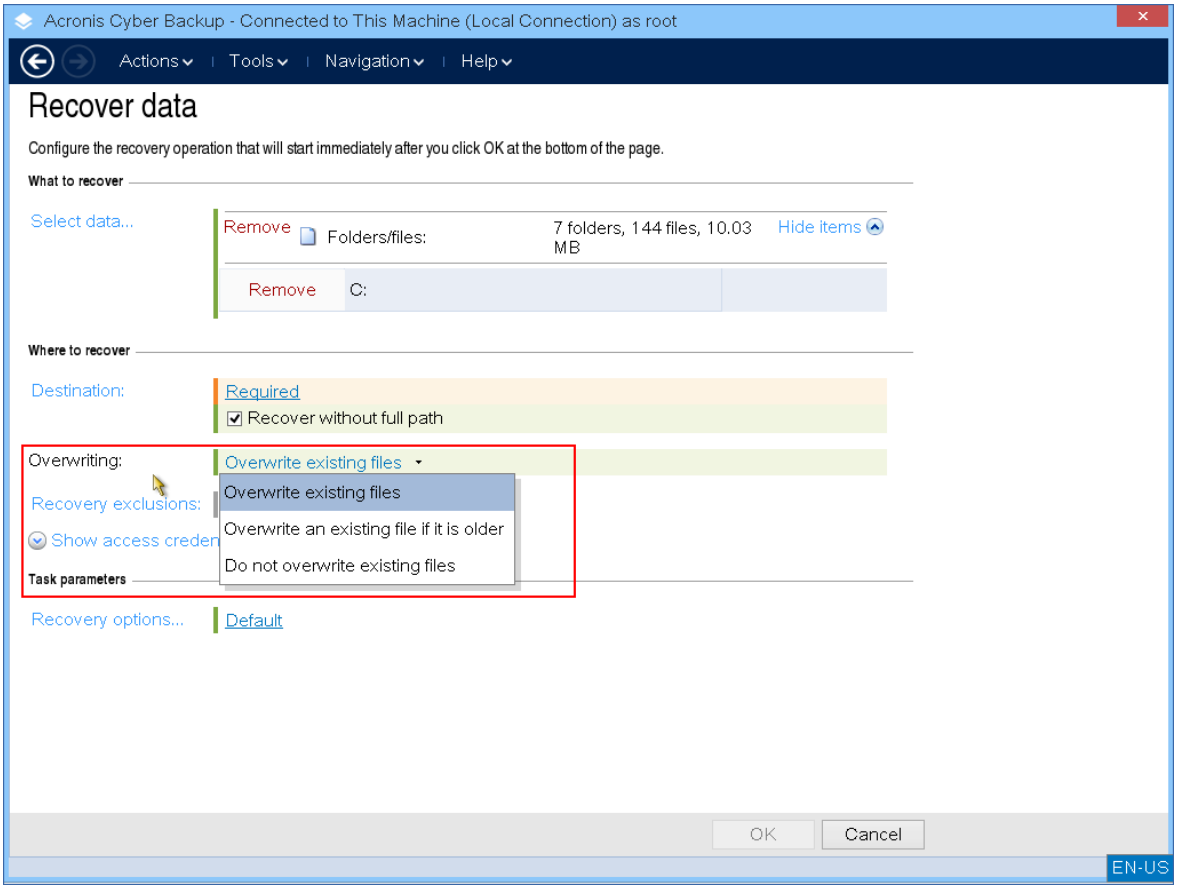
5. Kliknij **Przeglądaj** i wybierz lokalizację kopii zapasowej.



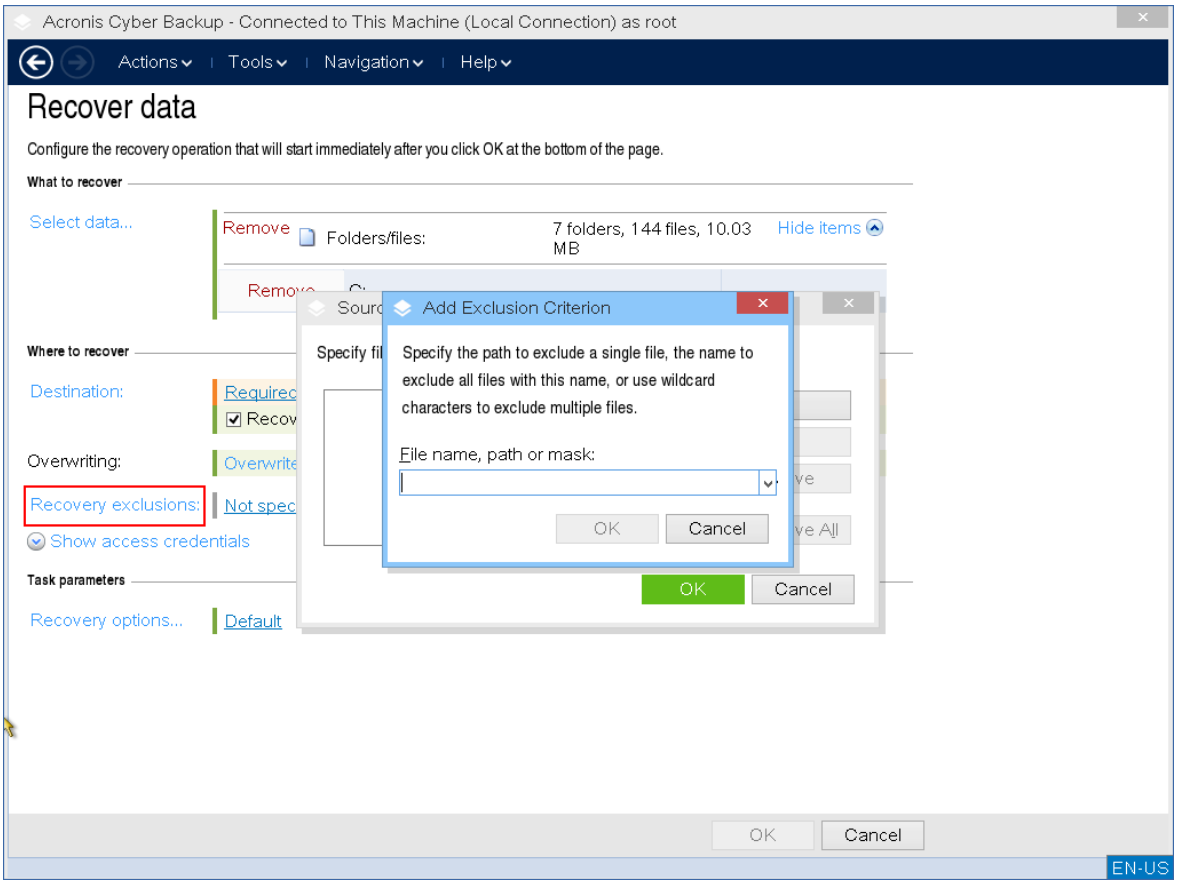
6. Wybierz plik kopii zapasowej, z którego chcesz odzyskać dane.



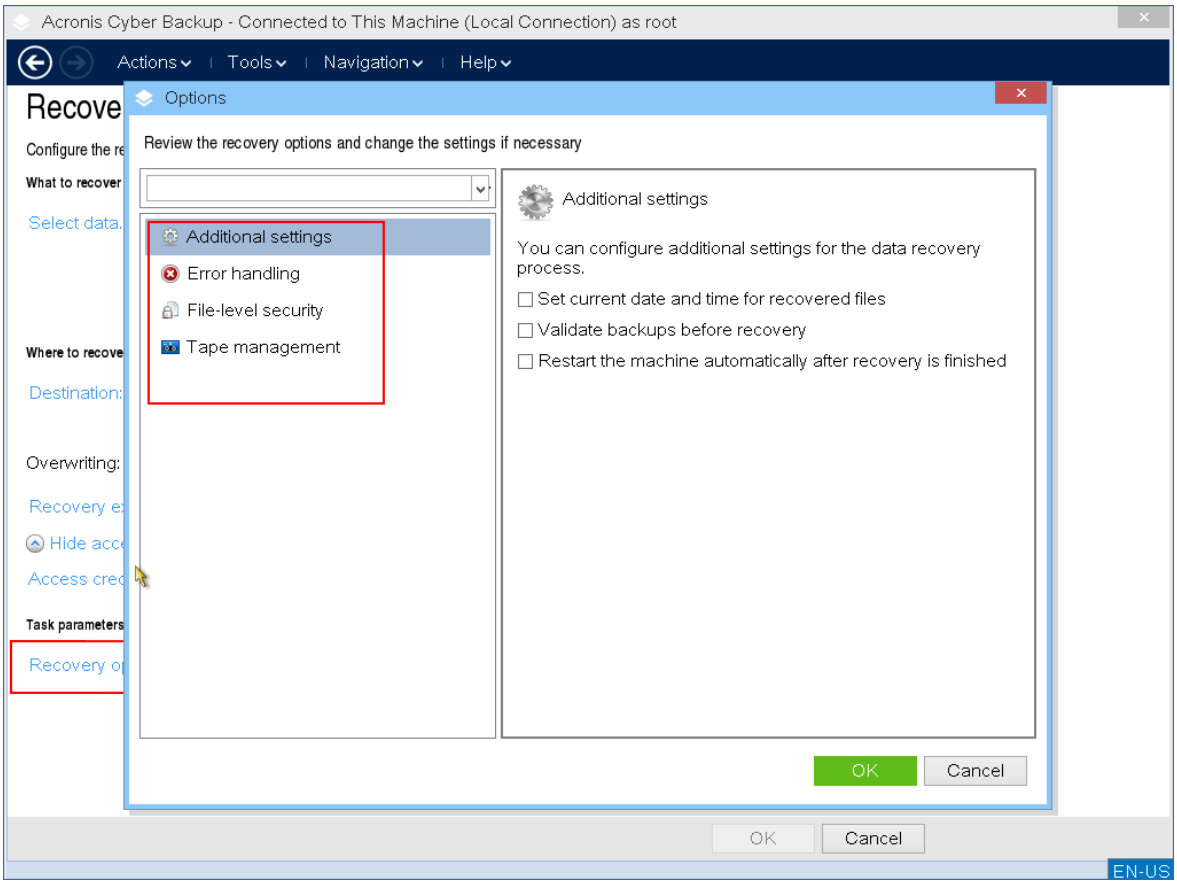
7. W lewym dolnym okienku wybierz dyski/wolumeny (lub pliki/foldery), które chcesz odzyskać, a następnie kliknij **OK**.
8. [Opcjonalnie] Skonfiguruj reguły zastępowania.



9. [Opcjonalnie] Skonfiguruj wykluczenia z odzyskiwania.



10. [Opcjonalnie] Skonfiguruj opcje odzyskiwania.



11. Sprawdź, czy ustawienia są prawidłowe, i kliknij **OK**.

Uwaga

Aby odzyskać dane w innej konfiguracji sprzętowej, trzeba skorzystać z usługi Acronis Universal Restore. Usługa
Acronis Universal Restore nie jest dostępna, jeśli kopia zapasowa znajduje się na partycji Acronis Secure Zone.

Zarządzanie dyskiem przy użyciu nośnika startowego

Za pomocą nośnika startowego Acronis można przygotować konfigurację dysku/woluminu pod kątem odzyskiwania obrazów woluminów uwzględnionych w kopii zapasowej za pomocą programu Acronis Cyber Protect.

Czasami po utworzeniu kopii zapasowej woluminu i umieszczeniu jego obrazu w bezpiecznym miejscu przechowywania konfiguracja dysków komputera może ulec zmianie z powodu wymiany dysku twardego lub utraty sprzętu. W takim przypadku można odtworzyć niezbędną konfigurację dysków. Pozwala to odzyskać obraz woluminu w dokładnie takiej postaci, jaką miał on wcześniej, lub wprowadzić dowolną niezbędną zmianę struktury dysków lub woluminów.

Aby uniknąć możliwej utraty danych, należy zastosować wszystkie niezbędne środki ostrożności.

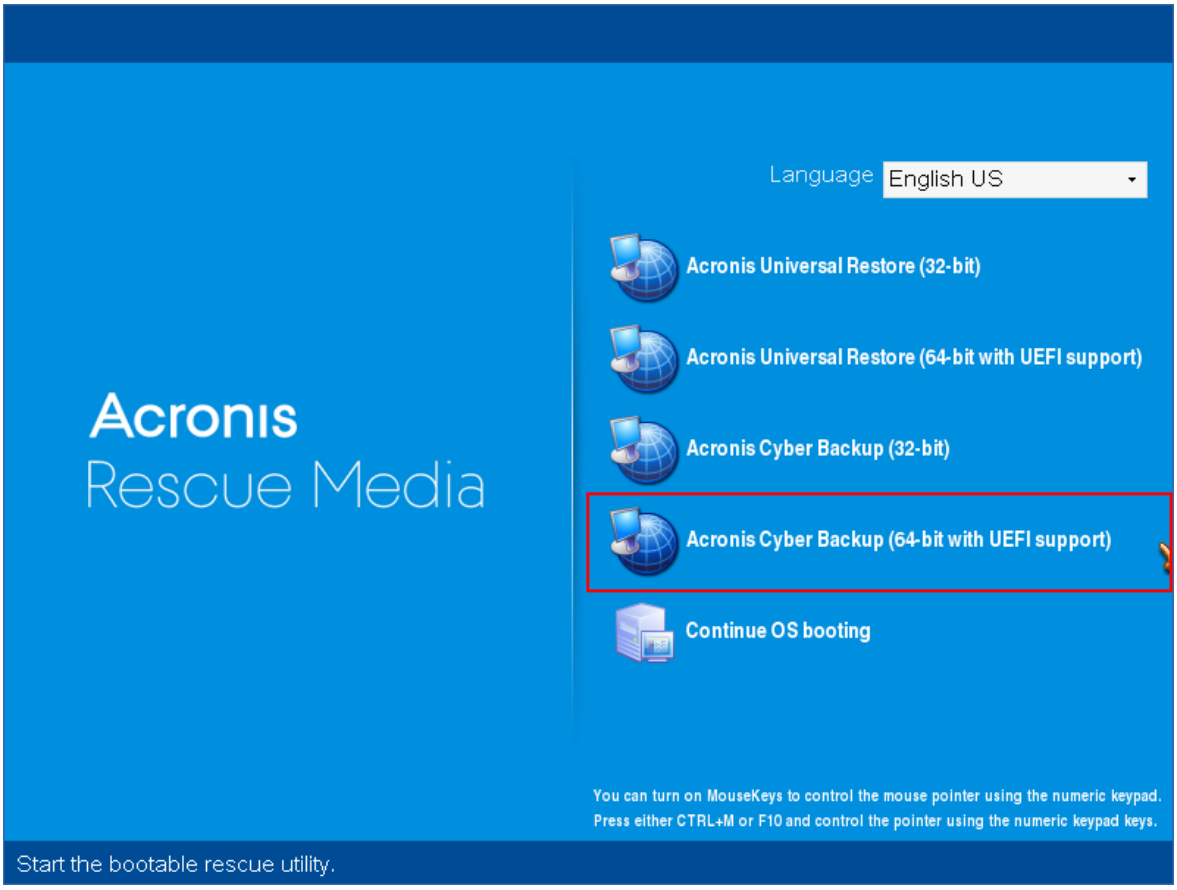
Ważne
Wszystkie operacje na dyskach i woluminach wiążą się z pewnym ryzykiem uszkodzenia danych. Operacje na woluminach systemowych, startowych lub woluminach danych należy wykonywać bardzo ostrożnie, aby uniknąć możliwych problemów z procesem uruchamiania lub przechowywaniem danych na dysku twardym.
Operacje na dyskach twardych i woluminach zajmują trochę czasu, a każda przerwa w zasilaniu, niezamierzone wyłączenie komputera lub przypadkowe naciśnięcie przycisku resetowania podczas wykonywania procedury może spowodować uszkodzenie woluminu i utratę danych.

Operacje zarządzania dyskiem można uruchomić na komputerze bez systemu operacyjnego, na komputerze, którego nie można uruchomić, a także na komputerze z systemem operacyjnym innym niż Windows. Będziesz potrzebować nośnika startowego utworzonego za pomocą narzędzia Bootable Media Builder oraz przy użyciu klucza licencyjnego programu Acronis Cyber Protect. Więcej informacji na temat tworzenia nośnika startowego można znaleźć w sekcji Nośnik startowy oparty na systemie Linux lub Nośnik startowy oparty na środowisku Windows PE.

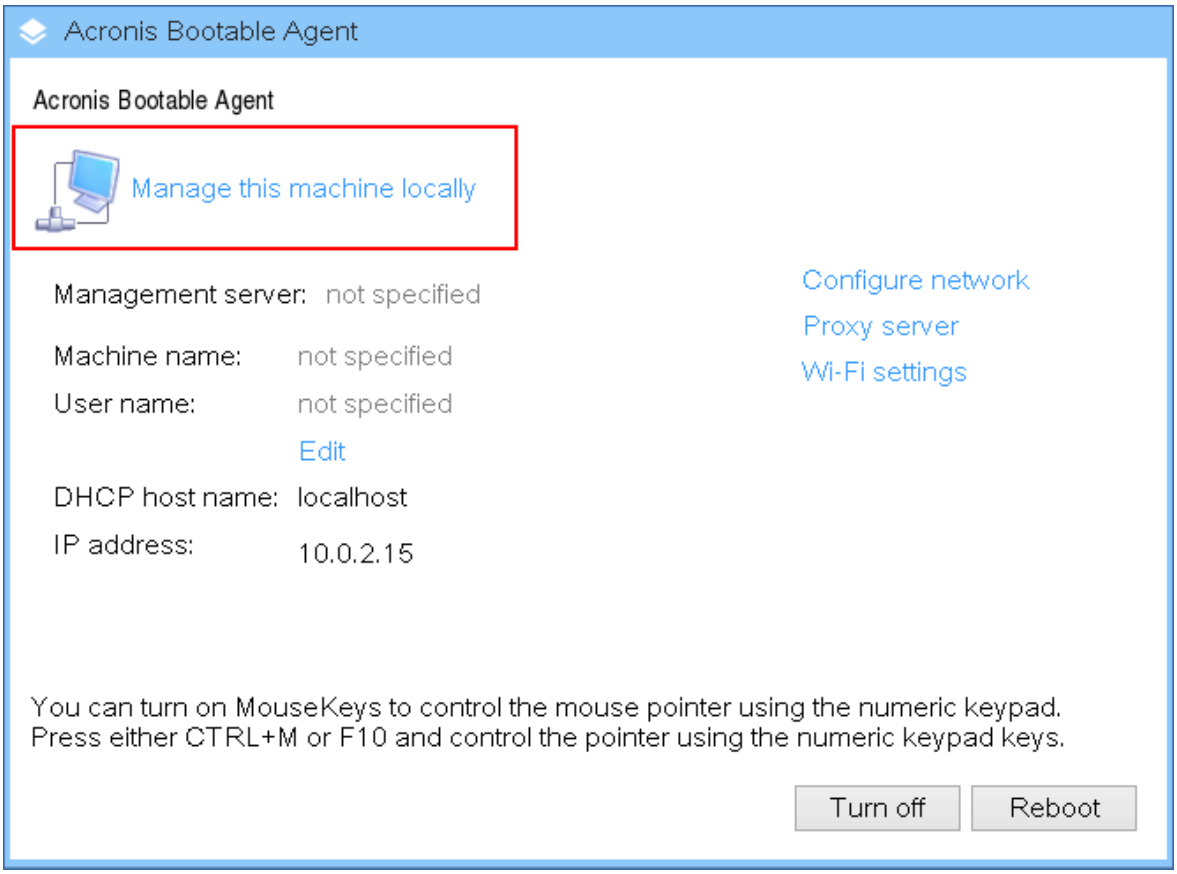
Uwaga
Funkcja zarządzania dyskami jest niedostępna dla nośników startowych opartych na środowisku WinPE w wersji 4.0. Funkcja zarządzania dyskami jest dostępna dla systemu operacyjnego Windows 7 i wcześniejszych wersji. Aby wykonywać operacje zarządzania dyskami w systemie operacyjnym Windows 8 i nowszym, należy zainstalować program Acronis Disk Director. Więcej informacji można znaleźć w następującym artykule bazy wiedzy: https://kb.acronis.com/content/47031.

Aby wykonać operacje zarządzania dyskami

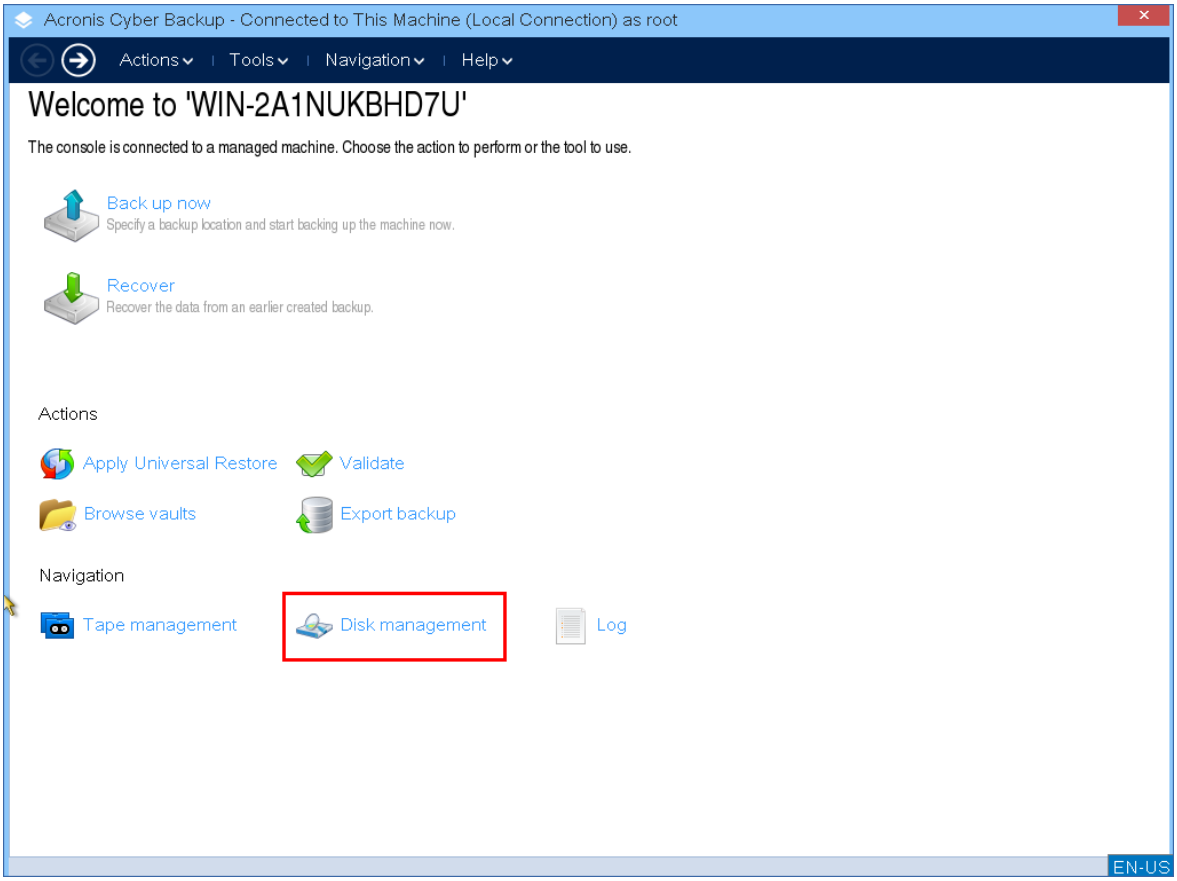
1. Uruchom z ratunkowego nośnika startowego firmy Acronis.



2. Aby pracować na komputerze lokalnym, kliknij **Zarządzaj tym komputerem lokalnie**. W przypadku połączeń zdalnych zobacz sekcję Rejestrowanie nośnika na serwerze zarządzania.



3. Kliknij **Zarządzanie dyskami**.



Uwaga
Operacje zarządzania dyskiem na nośnikach startowych mogą być wykonywane nieprawidłowo, jeśli na komputerze skonfigurowane są miejsca w pamięci masowej.

Obsługiwane systemy plików

Nośnik startowy obsługuje zarządzanie dyskami z następującymi systemami plików:

- FAT 16/32
- NTFS

Jeśli chcesz wykonać operacje na woluminie z innym systemem plików, użyj funkcji Acronis Disk Director. Oferuje ona więcej narzędzi umożliwiających zarządzanie dyskami i woluminami z następującymi systemami plików:

- FAT 16/32
- NTFS
- Ext2
- Ext3
- HFS+
- HFSX
- ReiserFS
- JFS
- Plik wymiany (SWAP) systemu Linux.

Podstawowe środki ostrożności

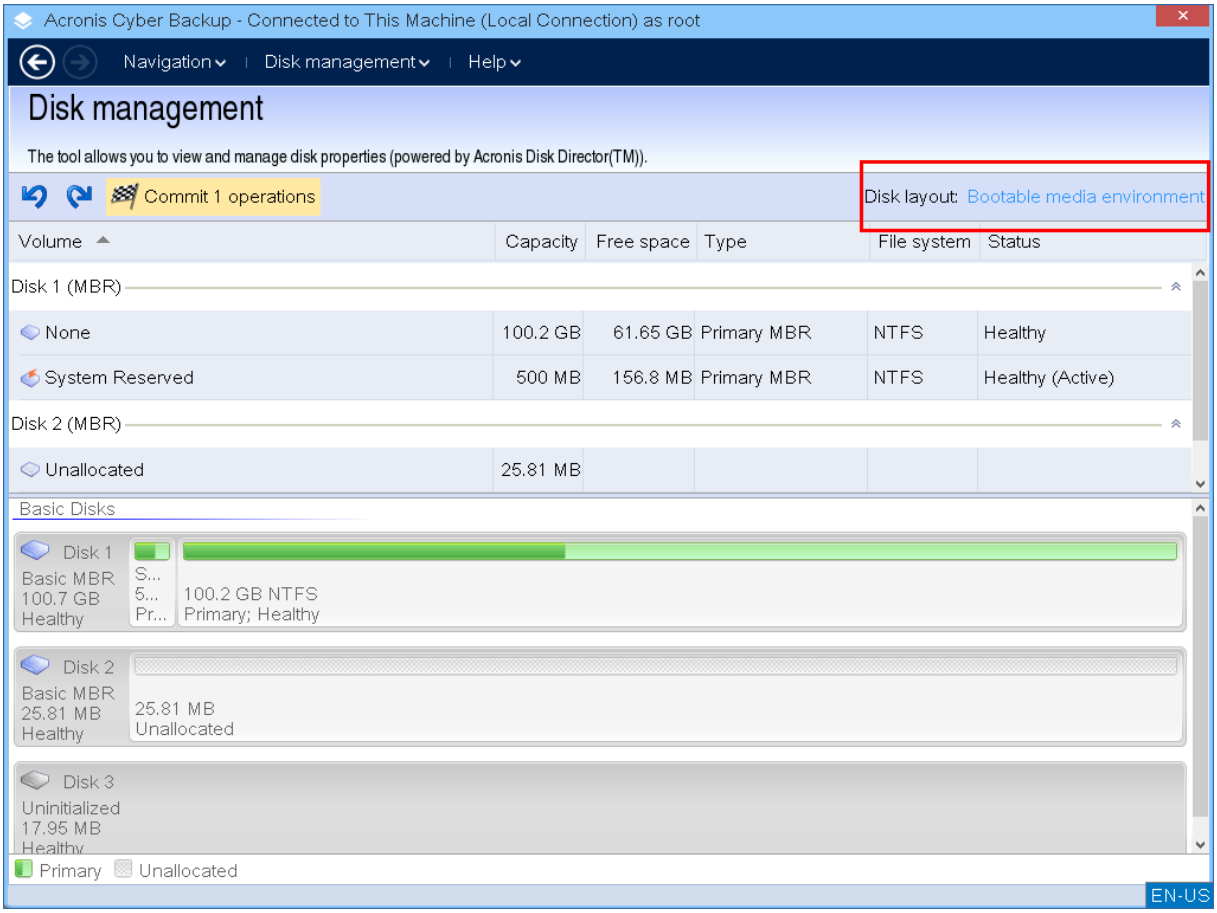
Aby uniknąć możliwego uszkodzenia struktury dysków i woluminów lub utraty danych, należy zastosować wszystkie niezbędne środki ostrożności oraz postępować zgodnie z następującymi wskazówkami:

1. Utwórz kopię zapasową dysku, na którym będzie się odbywało tworzenie woluminów lub zarządzanie nimi. Utworzenie kopii zapasowej najważniejszych danych na innym dysku twardym, w udziale sieciowym lub na nośniku wymiennym zagwarantuje bezpieczeństwo danych podczas pracy z woluminami dysku.
2. Sprawdź dysk, aby upewnić się, że jest w pełni sprawny i nie zawiera uszkodzonych sektorów ani błędów systemu plików.
3. Nie wykonuj żadnych operacji na dyskach/woluminach, gdy są uruchomione inne programy mające dostęp do dysków na niskim poziomie.

Wybieranie systemu operacyjnego do zarządzania dyskami

Na komputerze, na którym znajdują się co najmniej dwa systemy operacyjne, sposób przedstawiania dysków i woluminów zależy od aktualnie uruchomionego systemu operacyjnego. Ten sam wolumin może mieć przypisane różne w różnych systemach operacyjnych.

Aby wykonać operację zarządzania dyskami, należy określić układ dysku, dla którego będzie wyświetlany system operacyjny. W tym celu kliknij nazwę systemu operacyjnego obok etykiety **Układ dysku** i w otwartym oknie wybierz żądany system operacyjny.



Operacje na dyskach

Za pomocą nośnika startowego można wykonywać następujące operacje zarządzania dyskami:

- Inicjowanie dysku — inicjowanie nowego sprzętu dodanego do systemu.
- Klonowanie dysku standardowego — przenoszenie kompletnych danych ze źródłowego standardowego dysku MBR na dysk docelowy.
- Konwersja dysku: MBR na GPT — konwertowanie tabeli partycji MBR na GPT.
- Konwersja dysku: GPT na MBR — konwertowanie tabeli partycji GPT na MBR.
- Konwersja dysku: standardowy na dynamiczny — konwertowanie dysku standardowego na dysk dynamiczny.

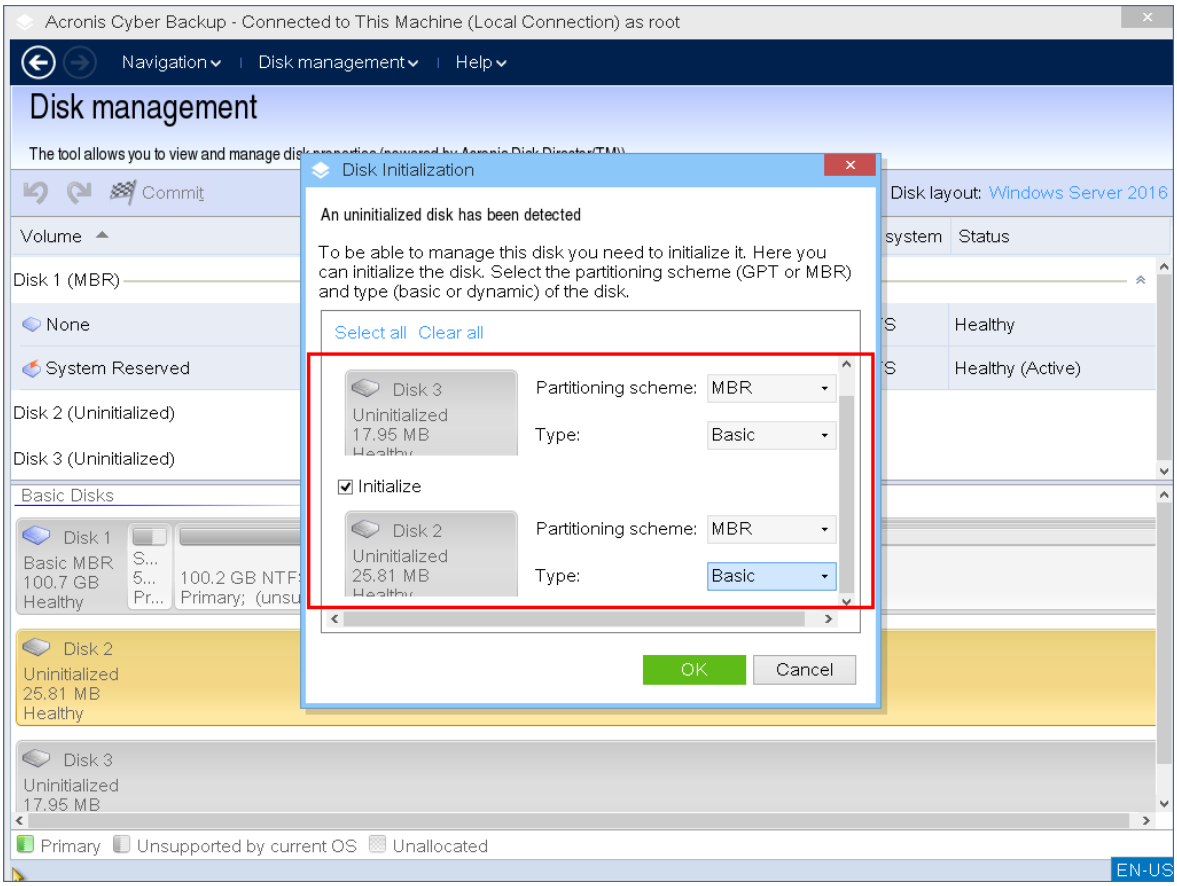
- Konwersja dysku: dynamiczny na standardowy — konwertowanie dysku dynamicznego na dysk standardowy.

Inicjowanie dysku

Nośnik startowy wyświetla niezainicjowany dysk w postaci szarego bloku z nieaktywną ikoną, co oznacza, że system nie może korzystać z tego dysku.

Aby zainicjować dysk

1. Kliknij prawym przyciskiem myszy żądany dysk i kliknij **Zainicjuj**.
2. W oknie **Inicjowanie dysku** ustaw schemat partycjonowania dysku (MBR lub GPT) oraz typ dysku (standardowy lub dynamiczny).
3. Kliknięcie przycisku **OK** spowoduje dodanie oczekującej operacji inicjowania dysku.
4. Aby ukończyć dodaną operację, wykonaj ją. Wyjście z programu bez wykonania operacji spowoduje jej skuteczne anulowanie.
5. Po zakończeniu inicjowania całe miejsce na dysku jest nieprzydzielone. Aby móc z niego skorzystać, trzeba na nim utworzyć wolumin.



Klonowanie dysku podstawowego

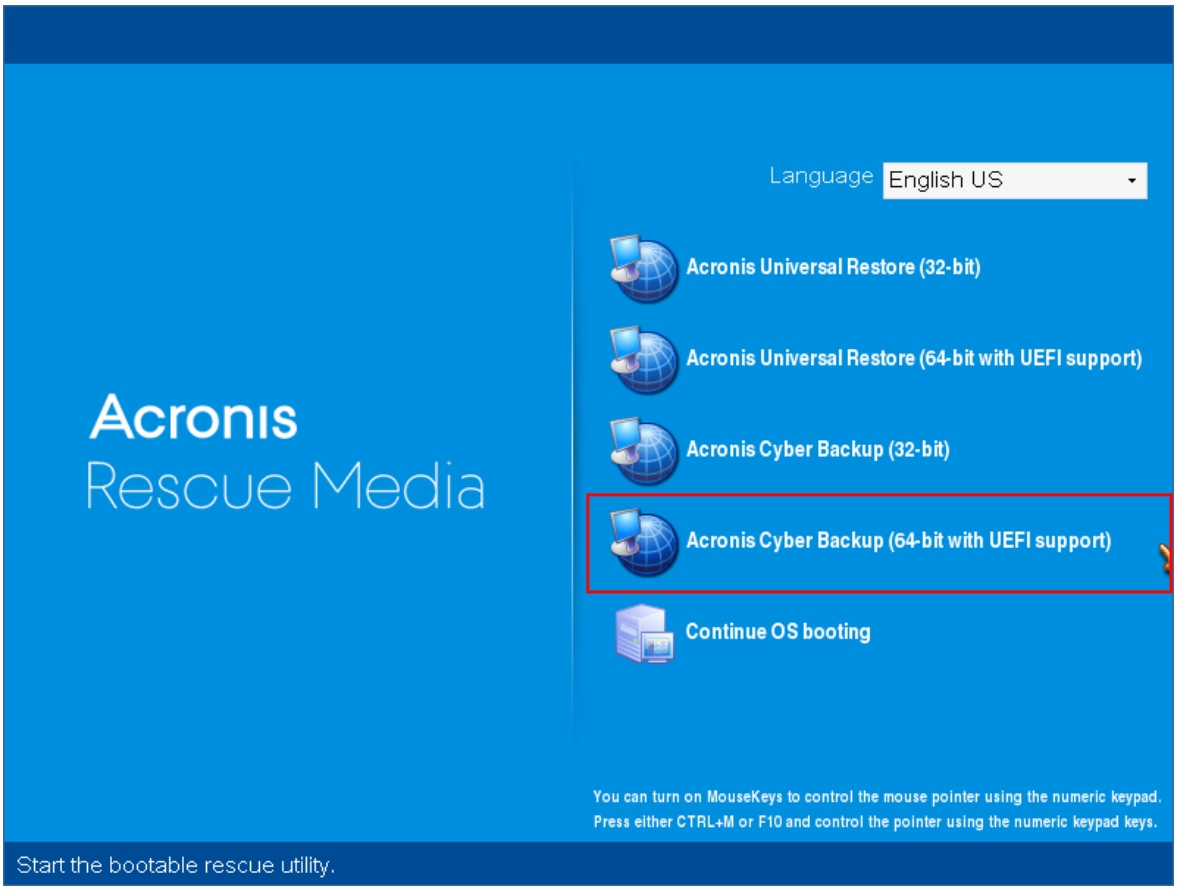
Za pomocą w pełni funkcjonalnego nośnika startowego opartego na systemie Linux można klonować standardowe dyski MBR. Funkcja klonowania dysków nie jest dostępna w przypadku

gotowego nośnika startowego, który można pobrać, ani w przypadku nośnika startowego, który jest tworzony bez klucza licencyjnego.

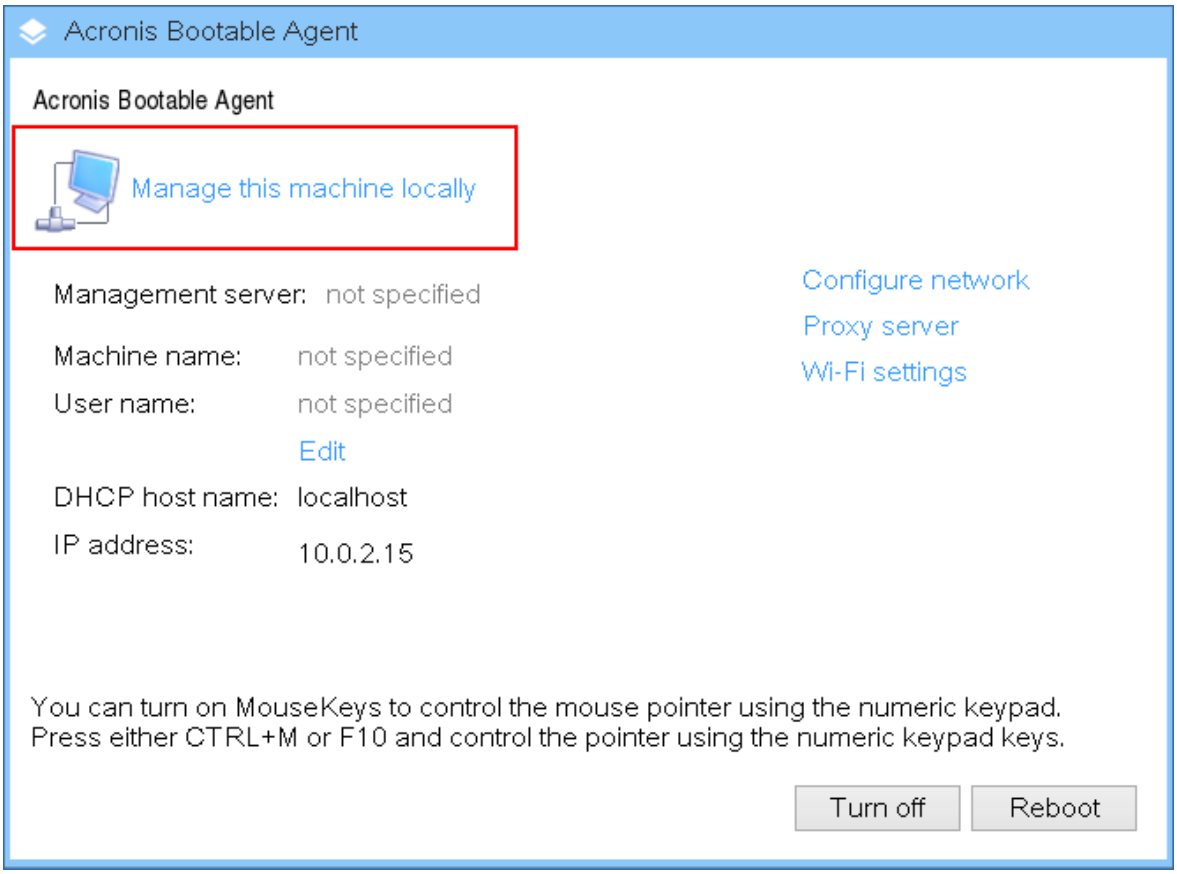
Uwaga
Dyski można też sklonować przy użyciu narzędzia wiersza polecenia programu Acronis Cyber Protect.

Aby sklonować dyski standardowe przy użyciu nośnika standardowego

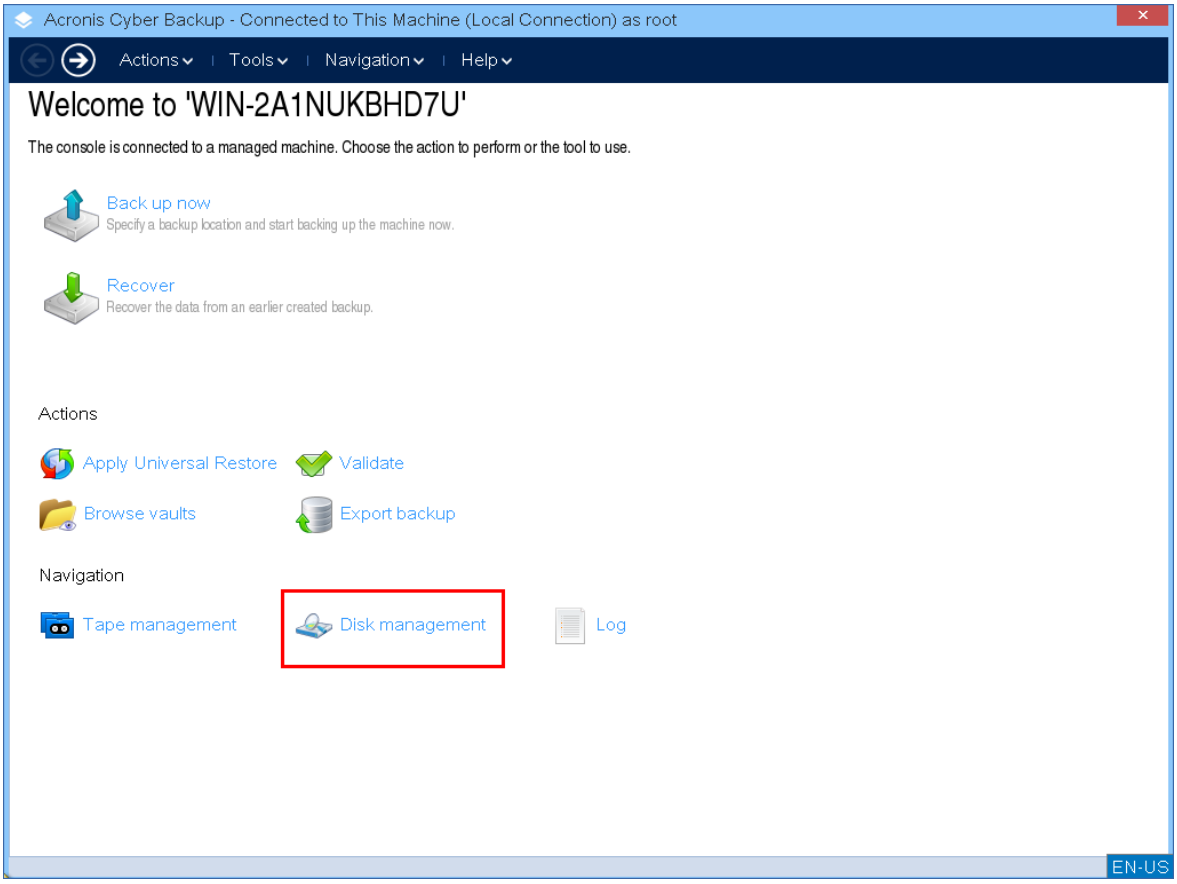
1. Uruchom z ratunkowego nośnika startowego firmy Acronis.



2. Aby sklonować dysk komputera lokalnego, kliknij **Zarządzaj tym komputerem lokalnie**. W przypadku połączenia zdalnego zobacz sekcję Rejestrowanie nośnika na serwerze zarządzania.

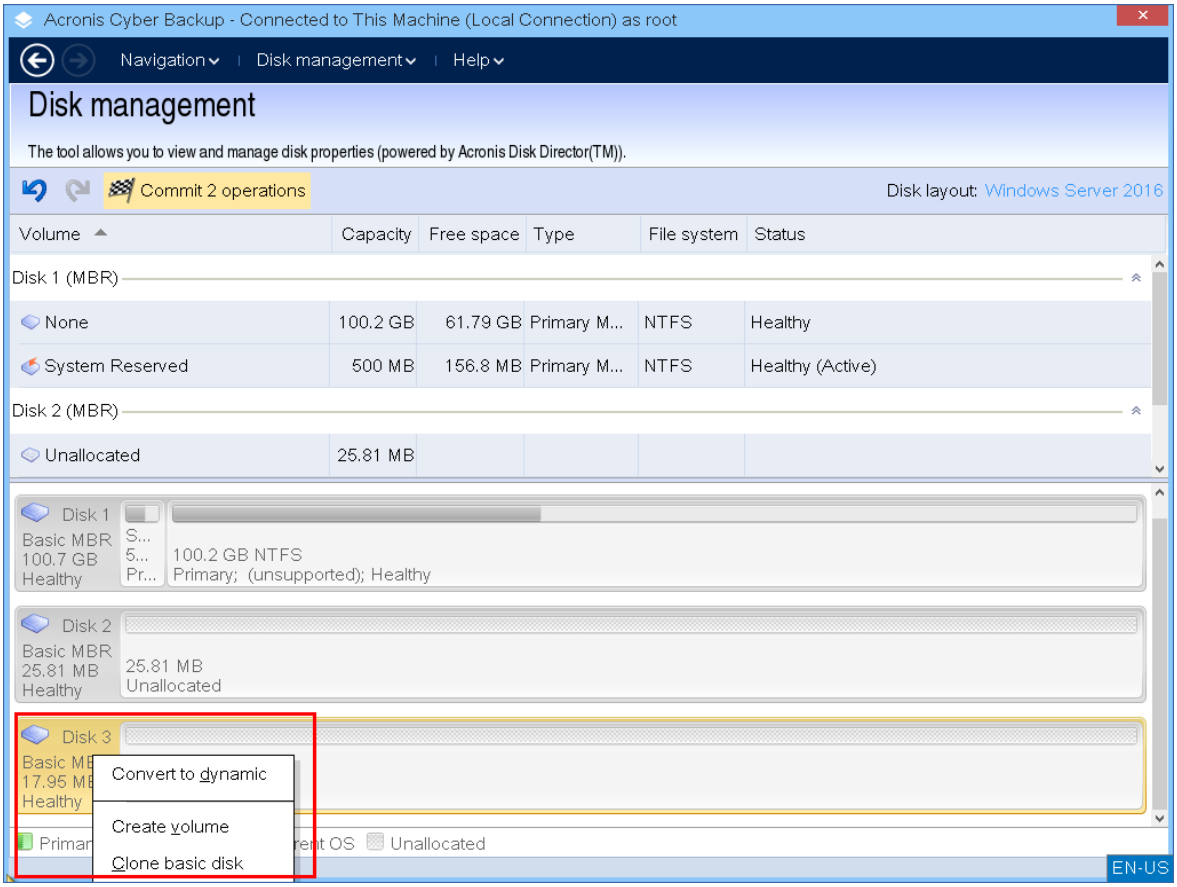


3. Kliknij **Zarządzanie dyskami**.

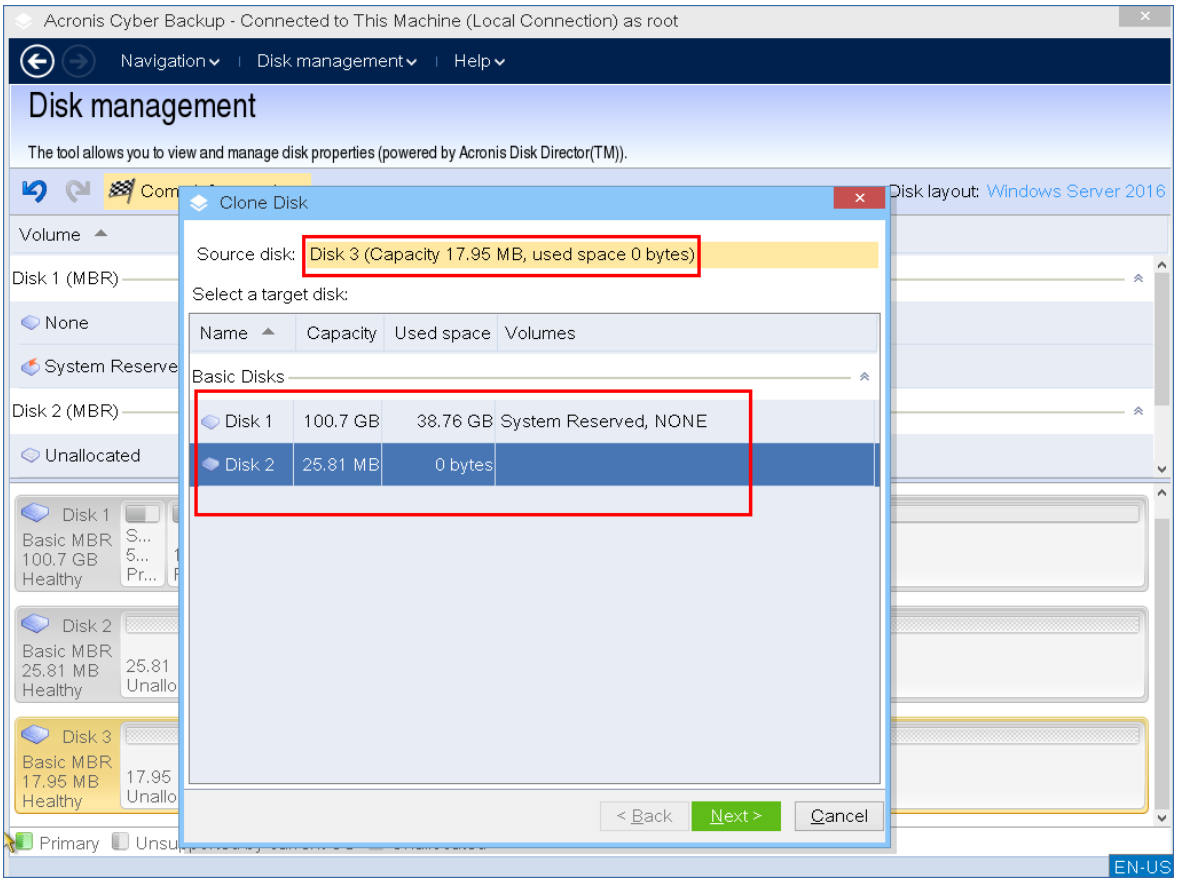


4. Zostaną wyświetlone dostępne dyski. Kliknij prawym przyciskiem myszy dysk, który chcesz sklonować, a następnie kliknij **Klonuj dysk podstawowy**.

Uwaga
Można klonować tylko całe dyski. Klonowanie partycji jest niedostępne.

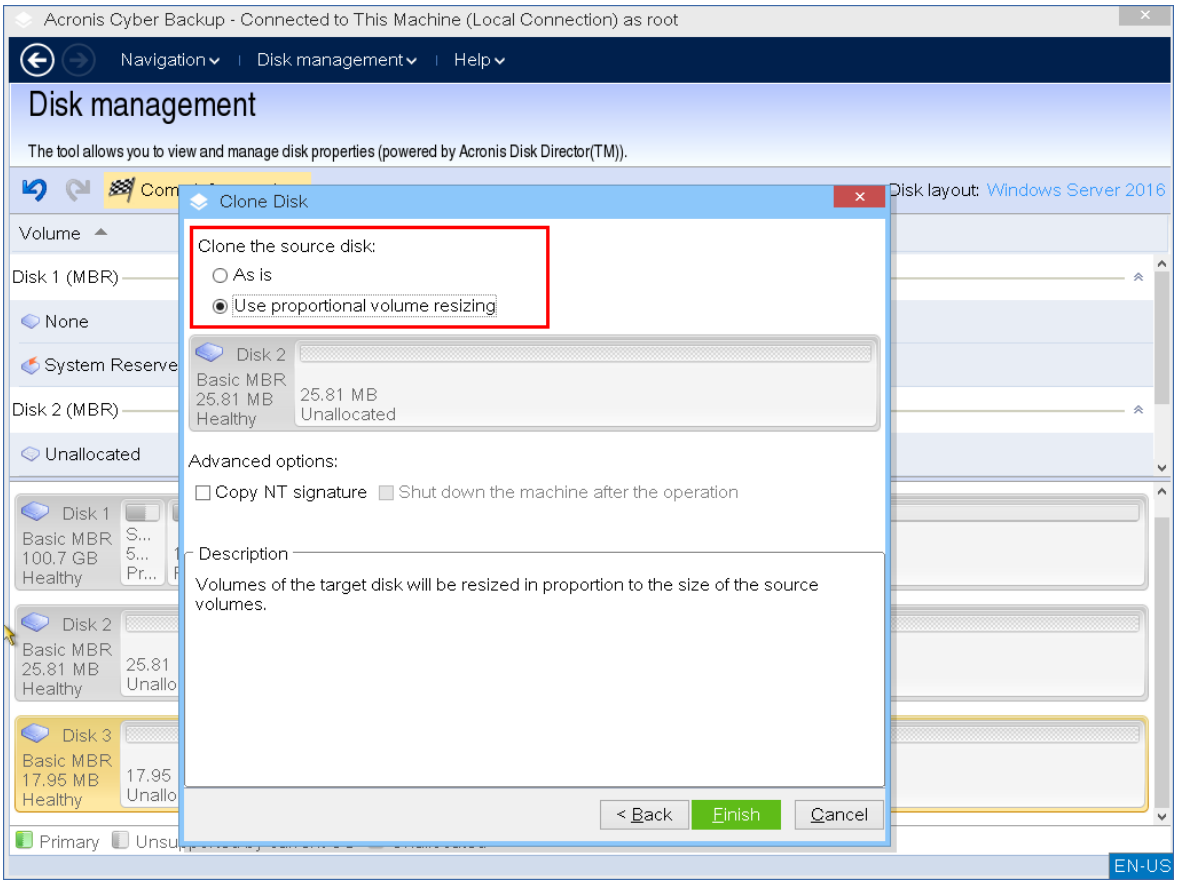


5. Wyświetlana jest lista potencjalnych dysków docelowych. Program umożliwia wybranie dysku docelowego, jeśli jest on wystarczająco duży, aby pomieścić wszystkie dane z dysku źródłowego — bez strat. Wybierz dysk docelowy i kliknij **Dalej**.

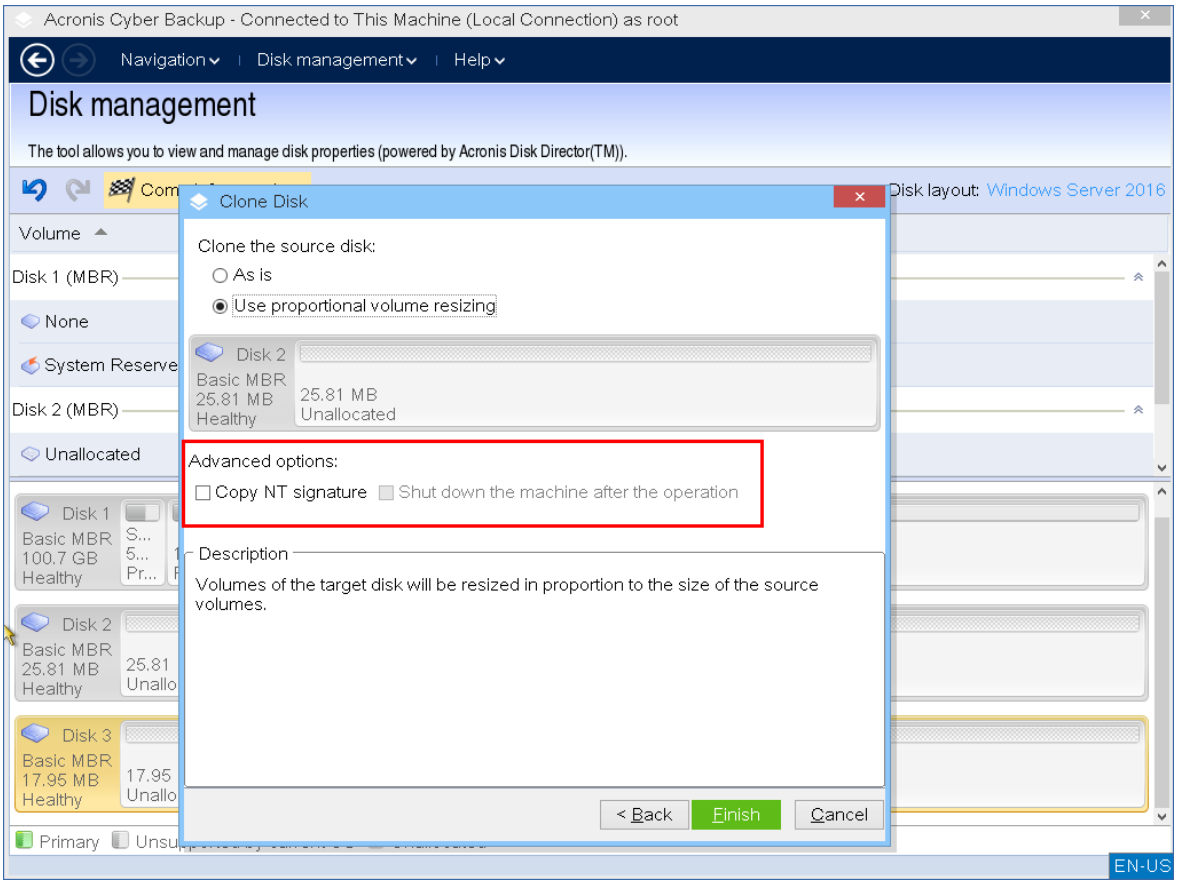


Jeśli dysk docelowy jest większy, można sklonować dysk w jego obecnej formie lub proporcjonalnie zmienić rozmiary woluminów (opcja domyślna), aby uniknąć pozostawienia na dysku docelowym nieprzydzielonego miejsca.
Jeśli dysk docelowy jest mniejszy, dostępna jest tylko opcja proporcjonalnej zmiany rozmiarów. Jeśli nie można bezpieczne wykonać klonowania nawet przy proporcjonalnej zmianie rozmiarów, nie będzie można kontynuować operacji.

Ważne
Jeśli na dysku docelowym znajdują się dane, pojawi się następujące ostrzeżenie: *„Wybrany dysk docelowy nie jest pusty. Dane w jego woluminach zostaną zastąpione”.* Jeśli będziesz kontynuować, wszystkie dane, które znajdują się obecnie na dysku docelowym, zostaną nieodwracalnie utracone.



6. Wybierz, czy ma zostać skopiowany podpis NT.



W przypadku klonowania dysku zawierającego wolumin systemowy trzeba zachować możliwość uruchamiania systemu operacyjnego na woluminie dysku docelowego. Oznacza to, że w systemie operacyjnym informacje o woluminie systemowym (na przykład litera woluminu) muszą pasować do podpisu NT dysku przechowywanego w jego rekordzie MBR. Jednak dwa dyski z tym samym podpisem NT nie mogą działać prawidłowo w jednym systemie operacyjnym.

Jeśli dwa dyski w komputerze mają ten sam podpis NT i zawierają wolumin systemowy, podczas rozruchu system operacyjny uruchamia się z pierwszego dysku, wykrywa taki sam podpis na drugim dysku, automatycznie generuje nowy, unikatowy podpis NT i przypisuje go do drugiego dysku. Wskutek tego wszystkie woluminy na drugim dysku tracą swoje litery, wszystkie ścieżki na dysku stają się nieprawidłowe, a programy nie mogą znaleźć swoich plików. Uruchomienie systemu operacyjnego umieszczonego na tym dysku jest niemożliwe.

Aby zachować możliwość uruchamiania systemu na woluminie dysku docelowego:

a. **Skopiuj podpis NT** — dysk docelowy otrzymuje podpis NT dysku źródłowego pasujący do kluczy rejestru także skopiowanych na dysk docelowy.

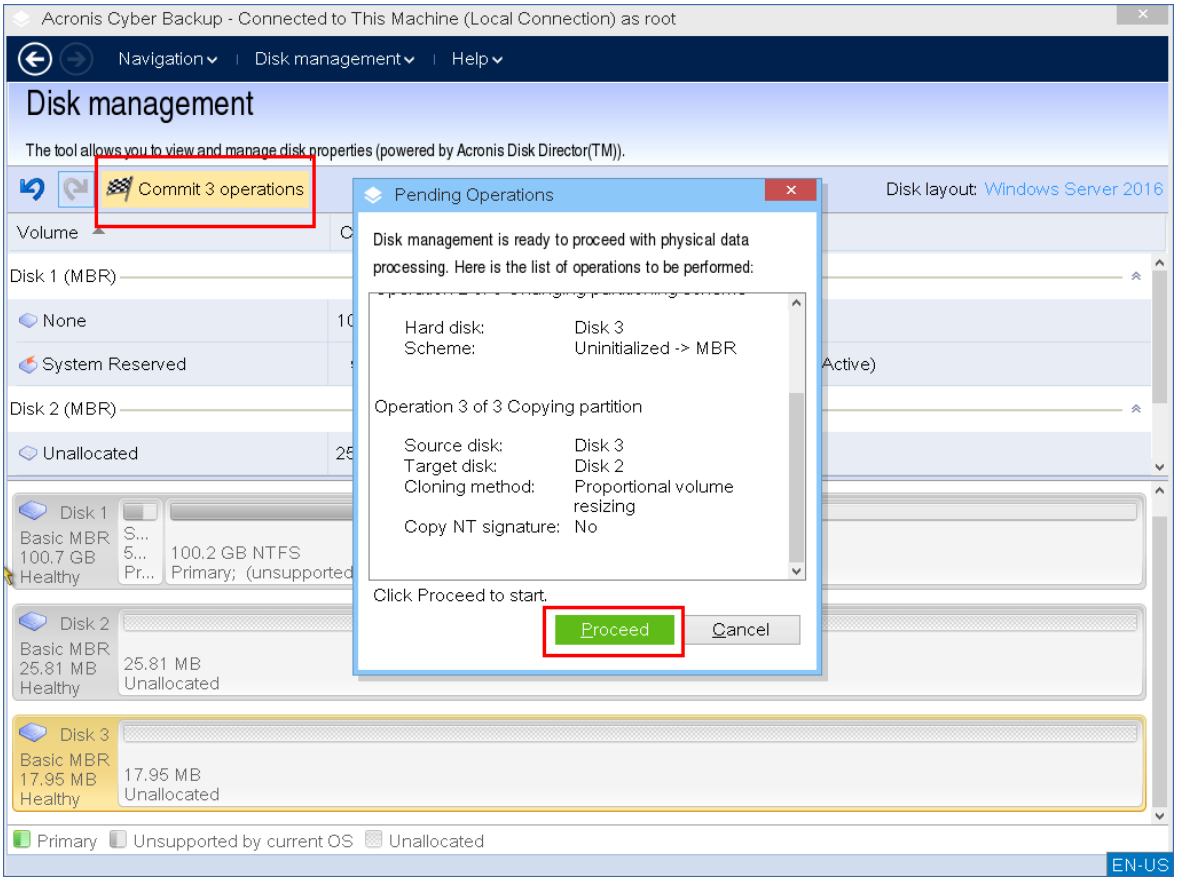
   W tym celu zaznacz pole wyboru **Kopiuj podpis NT**.

   Otrzymasz następujące ostrzeżenie: *„Jeśli na dysku twardym znajduje się system operacyjny, przed ponownym uruchomieniem należy odinstalować źródłowy lub docelowy dysk twardy komputera.W przeciwnym razie system operacyjny zostanie uruchomiony z pierwszego z nich, a systemu operacyjnego znajdującego się na drugim dysku nie będzie można uruchomić”.*

   Pole wyboru **Zamknij system komputera po operacji** zostanie automatycznie zaznaczone i wyłączone.

b. **Pozostaw podpis NT** — stary podpis dysku docelowego zostanie zachowany, a system operacyjny zostanie zaktualizowany odpowiednio do tego podpisu.
W tym celu w razie potrzeby kliknij pole wyboru **Kopiuj podpis NT**, aby je wyczyścić.
Pole wyboru **Zamknij system komputera po operacji** zostanie automatycznie wyczyszczone.

7. Kliknij **Zakończ**, aby dodać oczekującą operację klonowania dysków.
8. Kliknij **Wykonaj**, a następnie kliknij **Kontynuuj** w oknie **Operacje oczekujące**. Wyjście z programu bez wykonania operacji spowoduje jej skuteczne anulowanie.



9. Jeśli zdecydujesz się skopiować podpis NT, poczekaj, aż operacja zostanie zakończona i komputer zostanie wyłączony, a następnie odłącz źródłowy lub docelowy dysk twardy od komputera.

Konwersja dysku: MBR na GPT

Możesz przekonwertować standardowy dysk MBR na podstawowy standardowy GPT, jeśli potrzebujesz:

- Więcej niż 4 woluminów podstawowych na jednym dysku.
- Dodatkowej ochrony przed możliwym uszkodzeniem danych.

Ważne
Standardowego dysku MBR, który zawiera wolumin startowy z aktualnie uruchomionym systemem operacyjnym, nie można przekonwertować na dysk GPT.

Aby przekonwertować standardowy dysk MBR na standardowy dysk GPT

1. Kliknij prawym przyciskiem myszy dysk, który chcesz sklonować, a następnie kliknij **Konwertuj na GPT**.
2. Kliknięcie **OK** spowoduje dodanie oczekującej operacji konwersji dysku MBR na GPT.
3. Aby ukończyć dodaną operację, wykonaj ją. Wyjście z programu bez wykonania operacji spowoduje jej skuteczne anulowanie.

Uwaga
Dysk podzielony na partycje GPT rezerwuje na końcu obszaru partycji miejsce potrzebne na kopie zapasowe, w którym przechowywane są kopie nagłówka GPT i tabeli partycji. Jeśli dysk jest pełny i nie można automatycznie zmniejszyć rozmiaru woluminu, operacja konwersji dysku MBR na GPT zakończy się niepowodzeniem.
Ta operacja jest nieodwracalna. Jeśli wolumin podstawowy należący do dysku MBR zostanie przekonwertowany najpierw na dysk GPT, a następnie z powrotem na dysk MBR, stanie się woluminem logicznym i nie będzie można go używać jako woluminu systemowego.

Konwersja dysku dynamicznego: MBR na GPT

Nośnik startowy nie obsługuje bezpośredniej konwersji dysku MBR na GPT w przypadku dysków dynamicznych. Aby jednak osiągnąć ten cel, można wykonać następujące konwersje:

1. Konwersja dysku MBR: dynamiczny na standardowy przy użyciu operacji **Konwertuj na podstawowy**.
2. Konwersja dysku standardowego: MBR na GPT przy użyciu operacji **Konwertuj na GPT**.
3. Konwersja dysku GPT: standardowy na dynamiczny przy użyciu operacji **Konwertuj na dynamiczny**.

Konwersja dysku: GPT na MBR

Jeśli planujesz instalację systemu operacyjnego, który nie obsługuje dysków GPT, możesz przekonwertować dysk GPT na MBR.

Ważne
Standardowego dysku GPT, który zawiera wolumin startowy z aktualnie uruchomionym systemem operacyjnym, nie można przekonwertować na dysk MBR.

Aby przekonwertować dysk GPT na MBR

1. Kliknij prawym przyciskiem myszy dysk, który chcesz sklonować, a następnie kliknij **Konwertuj na MBR**.
2. Kliknięcie **OK** spowoduje dodanie oczekującej operacji konwersji dysku GPT na MBR.
3. Aby ukończyć dodaną operację, wykonaj ją. Wyjście z programu bez wykonania operacji spowoduje jej skuteczne anulowanie.

Uwaga
Po operacji woluminy na tym dysku stają się woluminami logicznymi. Tej zmiany nie można cofnąć.

Konwersja dysku: podstawowy na dynamiczny

Może być wskazana konwersja dysku standardowego na dynamiczny, jeśli:

- Dysk ma wchodzić w skład grupy dysków dynamicznych.
- Jest potrzebna dodatkowa ochrona danych przechowywanych na dysku.

Aby przekonwertować dysk standardowy na dynamiczny

1. Kliknij prawym przyciskiem myszy dysk, który chcesz przekonwertować, a następnie kliknij **Konwertuj na dynamiczny**.
2. Kliknij **OK**.

Konwersja zostanie wykonana niezwłocznie i w razie potrzeby komputer zostanie uruchomiony ponownie.

Uwaga
Dysk dynamiczny zajmuje ostatni megabajt dysku fizycznego w celu przechowywania bazy danych, która zawiera czteropoziomowy opis każdego woluminu dynamicznego (Wolumin-Komponent-Partycja-Dysk). Jeśli podczas konwersji dysku na dynamiczny okaże się, że dysk standardowy jest pełny i nie można automatycznie zmniejszyć rozmiaru jego woluminów, operacja konwersji dysku standardowego na dynamiczny się nie powiedzie.
Konwersja dysków zawierających woluminy systemowe zajmuje trochę czasu, a każda przerwa w zasilaniu, niezamierzone wyłączenie komputera lub przypadkowe naciśnięcie przycisku resetowania podczas wykonywania procedury może uniemożliwić uruchomienie systemu.

W odróżnieniu od Menedżera dysków systemu Windows umożliwia uruchomienie po zakończeniu operacji **systemu operacyjnego offline** znajdującego się na dysku.

Konwersja dysku: dynamiczny na podstawowy

Konwersja dysków dynamicznych na standardowe może być konieczna na przykład w przypadku, gdy chcesz rozpocząć korzystanie z systemu operacyjnego, który nie obsługuje dysków dynamicznych.

Aby przekonwertować dysk dynamiczny na standardowy:

1. Kliknij prawym przyciskiem myszy dysk, który chcesz przekonwertować, a następnie kliknij **Konwertuj na podstawowy**.
2. Kliknij **OK**.

Konwersja zostanie wykonana niezwłocznie i w razie potrzeby komputer zostanie uruchomiony ponownie.

Uwaga
Ta operacja nie jest dostępna w przypadku dysków dynamicznych zawierających woluminy łączone, rozłożone lub RAID-5.

Po zakończeniu konwersji ostatnie 8 MB miejsca na dysku jest rezerwowane na potrzeby przyszłej konwersji dysku standardowego na dynamiczny. W niektórych przypadkach możliwe nieprzydzielone miejsce i proponowany maksymalny rozmiar woluminu mogą się różnić (na przykład wtedy, gdy rozmiar jednego woluminu lustrzanego określa rozmiar drugiego lub gdy ostatnie 8 MB miejsca na dysku zostaje zarezerwowane na potrzeby przyszłej konwersji dysku standardowego na dynamiczny).

Uwaga
Konwersja dysków obejmująca woluminy systemowe trwa jakiś czas, a każda przerwa w zasilaniu, niezamierzone wyłączenie komputera lub przypadkowe naciśnięcie przycisku resetowania podczas wykonywania procedury może uniemożliwić uruchomienie systemu.

W odróżnieniu od Menedżera dysków systemu Windows program zapewnia:

- Bezpieczną konwersję dysku dynamicznego na standardowy, gdy zawiera on woluminy **z danymi** woluminów prostych i lustrzanych
- Na komputerach z funkcją uruchamiania wielu systemów operacyjnych: możliwość uruchomienia systemu, który w czasie operacji znajdował się w trybie **offline**

Operacje na woluminach

Za pomocą nośnika startowego można wykonywać następujące operacje dotyczące woluminów:

- Utwórz wolumin — umożliwia utworzenie nowego woluminu.
- Usuń wolumin — umożliwia usunięcie wybranego woluminu.
- Ustaw jako aktywny — umożliwia ustawienie wybranego woluminu jako aktywnego, aby umożliwić uruchamianie na komputerze systemu operacyjnego zainstalowanego na tym woluminie.
- Zmień literę — umożliwia zmianę litery wybranego woluminu.
- Zmień etykietę — umożliwia zmianę etykiety wybranego woluminu.
- Formatuj wolumin — umożliwia sformatowanie woluminu z zastosowaniem systemu plików.

Typy woluminów dynamicznych

Wolumin prosty

Wolumin utworzony z wolnego miejsca na jednym dysku fizycznym. Może on się składać z jednego regionu na dysku lub z kilku regionów połączonych wirtualnie przez Menedżera dysków

logicznych (LDM). Nie zapewnia większej niezawodności, większej szybkości ani dodatkowego miejsca.

Wolumin łączony

Wolumin utworzony z wolnego miejsca z kilku dysków fizycznych połączonego wirtualnie przez LDM. Na jednym woluminie można umieścić do 32 dysków, co pozwala na pokonanie ograniczeń sprzętowych. Jeśli jednak choć jeden dysk ulegnie awarii, wszystkie dane zostaną utracone. Ponadto nie można usunąć żadnej części woluminu łączonego tak, aby nie uszkodzić całego woluminu. Wolumin łączony nie zapewnia ani dodatkowej niezawodności, ani lepszych wskaźników operacji We/Wy.

Wolumin rozłożony

Taki wolumin, nazywany też woluminem RAID-0, składa się z pasów danych o takim samym rozmiarze zapisanych na każdym dysku woluminu. Oznacza to, że aby utworzyć wolumin rozłożony, potrzeba co najmniej dwóch dysków dynamicznych. Dyski woluminu rozłożonego nie muszą być takie same, ale na każdym z nich musi być dostępne wolne miejsce, które chcesz uwzględnić w woluminie. Rozmiar woluminu zależy od rozmiaru najmniejszej uwzględnionej przestrzeni dyskowej. Dostęp do danych na woluminie rozłożonym jest zwykle szybszy niż dostęp do tych samych danych na jednym dysku fizycznym, ponieważ wskaźnik We/Wy rozkłada się na więcej niż jeden dysk.

Woluminy rozłożone tworzy się w celu zwiększenia wydajności, a nie ze względu na większą niezawodność — nie zawierają one nadmiarowych informacji.

Wolumin lustrzany

Wolumin odporny na uszkodzenia, nazywany też woluminem RAID 1, którego dane są duplikowane na dwóch takich samych dyskach fizycznych. Wszystkie dane znajdujące się na jednym dysku są kopiowane na drugi dysk, aby zapewnić nadmiarowość danych. Niemal każdy wolumin można zduplikować wraz z woluminem systemowym i startowym. W przypadku awarii jednego dysku dane są dostępne na drugim. Niestety w przypadku korzystania z woluminów lustrzanych sprzętowe ograniczenia rozmiaru i wydajności są jeszcze większe.

Wolumin lustrzany-rozłożony

Wolumin odporny na uszkodzenia (określany czasem jako RAID 1+0), który łączy w sobie atut dużej szybkości operacji We/Wy występującej w układzie rozłożonym z nadmiarowością, jaką zapewnia układ lustrzany. Wadą wynikającą z architektury lustrzanej jest niski współczynnik rozmiaru dysku do rozmiaru woluminu.

RAID-5

Wolumin odporny na uszkodzenia, którego dane są rozłożone na co najmniej trzech dyskach. Dyski tego woluminu nie muszą być takie same, ale na każdym z nich muszą się znajdować równej wielkości bloki nieprzydzielonego miejsca. Również parzystość (obliczana wartość, której

można użyć do rekonstrukcji danych w przypadku uszkodzenia) jest rozłożona na całą macierz dysków. Ponadto jest ona zawsze przechowywana na innym dysku niż same dane. W przypadku awarii dysku fizycznego, część woluminu RAID-5 znajdująca się na uszkodzonym dysku może zostać odtworzona na podstawie pozostałych danych i parzystości. Wolumin RAID-5 zapewnia niezawodność i umożliwia przekroczenie ograniczeń związanych z rozmiarem dysku fizycznego dzięki wyższemu wskaźnikowi dysk lustrzany/rozmiar woluminu.

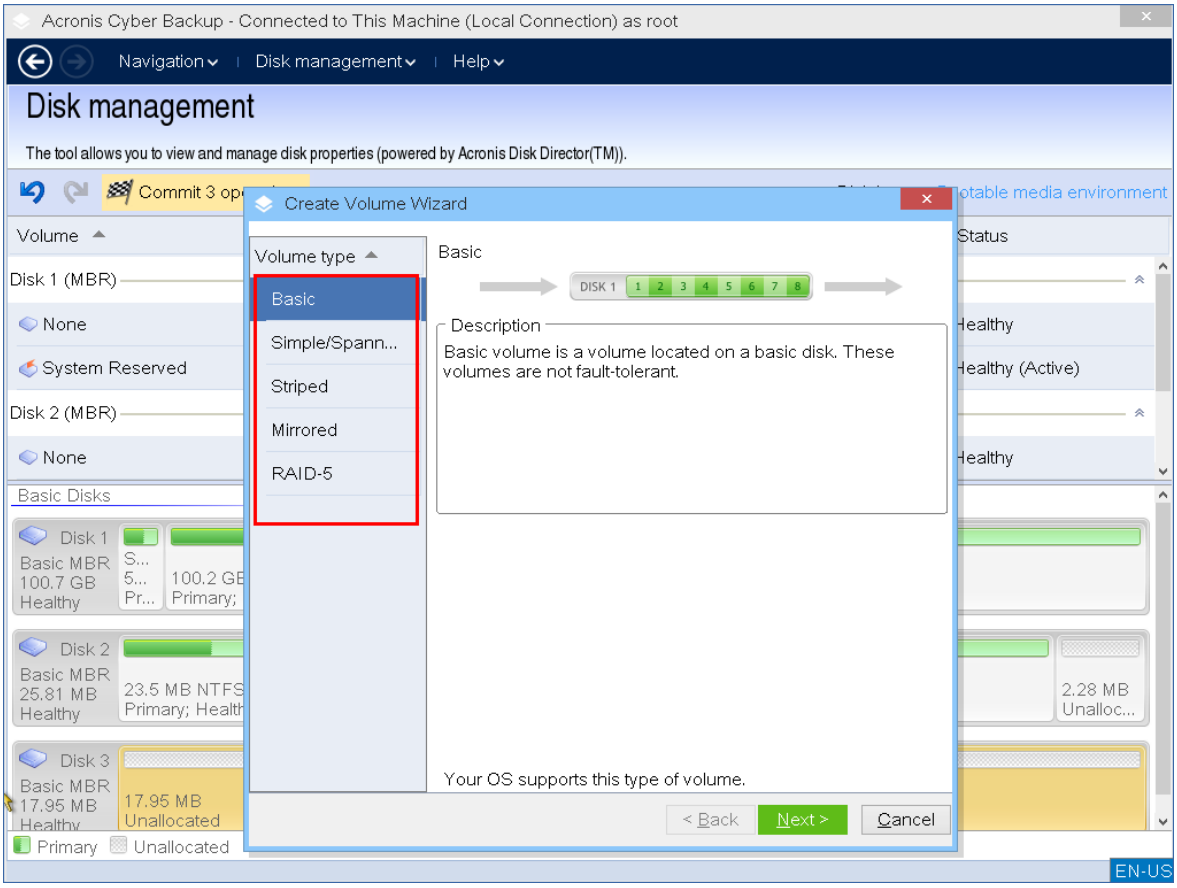
Utwórz wolumin

Nowy wolumin może być potrzebny do:

- odzyskania wcześniej zapisanej kopii zapasowej w identycznej postaci;
- oddzielnego przechowywania kolekcji podobnych plików, na przykład kolekcji plików MP3 lub wideo na oddzielnym woluminie
- przechowywania na specjalnym woluminie kopii zapasowych (obrazów) innych woluminów/dysków;
- zainstalowania nowego systemu operacyjnego (lub pliku wymiany) na nowym woluminie;
- dodania nowego sprzętu do komputera.

Aby utworzyć wolumin

1. Kliknij prawym przyciskiem myszy dowolne nieprzydzielone miejsce na dysku, a następnie kliknij **Utwórz wolumin**. Zostanie otwarty **Kreator tworzenia woluminów**.



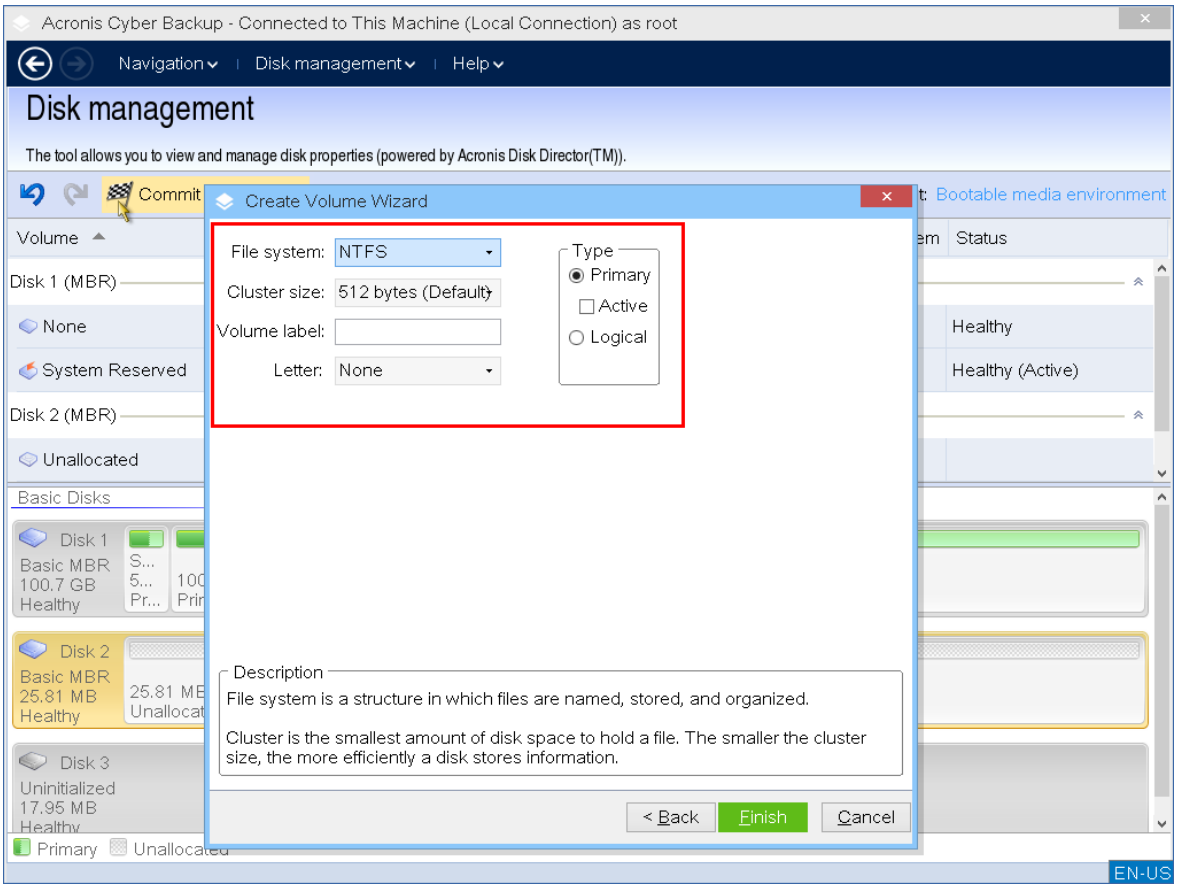
2. Wybierz typ woluminu. Dostępne są następujące opcje:
   - Podstawowy
   - Prosty/łączony
   - Rozłożony
   - Lustrzany
   - RAID-5

   Jeśli bieżący system operacyjny nie obsługuje wybranego typu woluminu, zostanie wyświetlone odpowiednie ostrzeżenie, a przycisk **Dalej** zostanie wyłączony. Aby kontynuować, trzeba będzie wybrać inny typ woluminu.
3. Określ nieprzydzielone miejsce lub wybierz dyski docelowe.
   - W przypadku woluminu standardowego określ nieprzydzielone miejsce na wybranym dysku.
   - W przypadku woluminu prostego/łączonego wybierz jeden lub więcej dysków docelowych.
   - W przypadku woluminu lustrzanego wybierz dwa dyski docelowe.
   - W przypadku woluminu rozłożonego wybierz dwa lub więcej dysków docelowych.
   - W przypadku woluminu RAID-5 wybierz trzy dyski docelowe.

   Jeśli tworzysz wolumin **dynamiczny** i jako jego miejsce docelowe wybierzesz jeden lub kilka dysków **podstawowych**, pojawi się ostrzeżenie, że wybrany dysk zostanie automatycznie przekonwertowany na dynamiczny.
4. Ustaw rozmiaru woluminu.

   Maksymalna wartość zazwyczaj odzwierciedla możliwą maksymalną ilość nieprzydzielonego miejsca. W niektórych przypadkach proponowana maksymalna wartość może być inna (na przykład wtedy, gdy rozmiar jednego woluminu lustrzanego określa rozmiar drugiego lub gdy ostatnie 8 MB miejsca na dysku zostaje zarezerwowane na potrzeby przyszłej konwersji dysku standardowego na dynamiczny).

   Jeśli nieprzydzielone miejsce na dysku jest większe niż wolumin, możesz wybrać położenie nowego woluminu standardowego.
5. Ustaw opcje woluminu.



Możesz przypisać woluminowi **literę** (domyślnie: pierwsza wolna litera alfabetu) i — opcjonalnie — **etykietę** (domyślnie: brak). Musisz też wskazać **System plików** oraz **Rozmiar klastra**.

Możliwe opcje systemu plików:

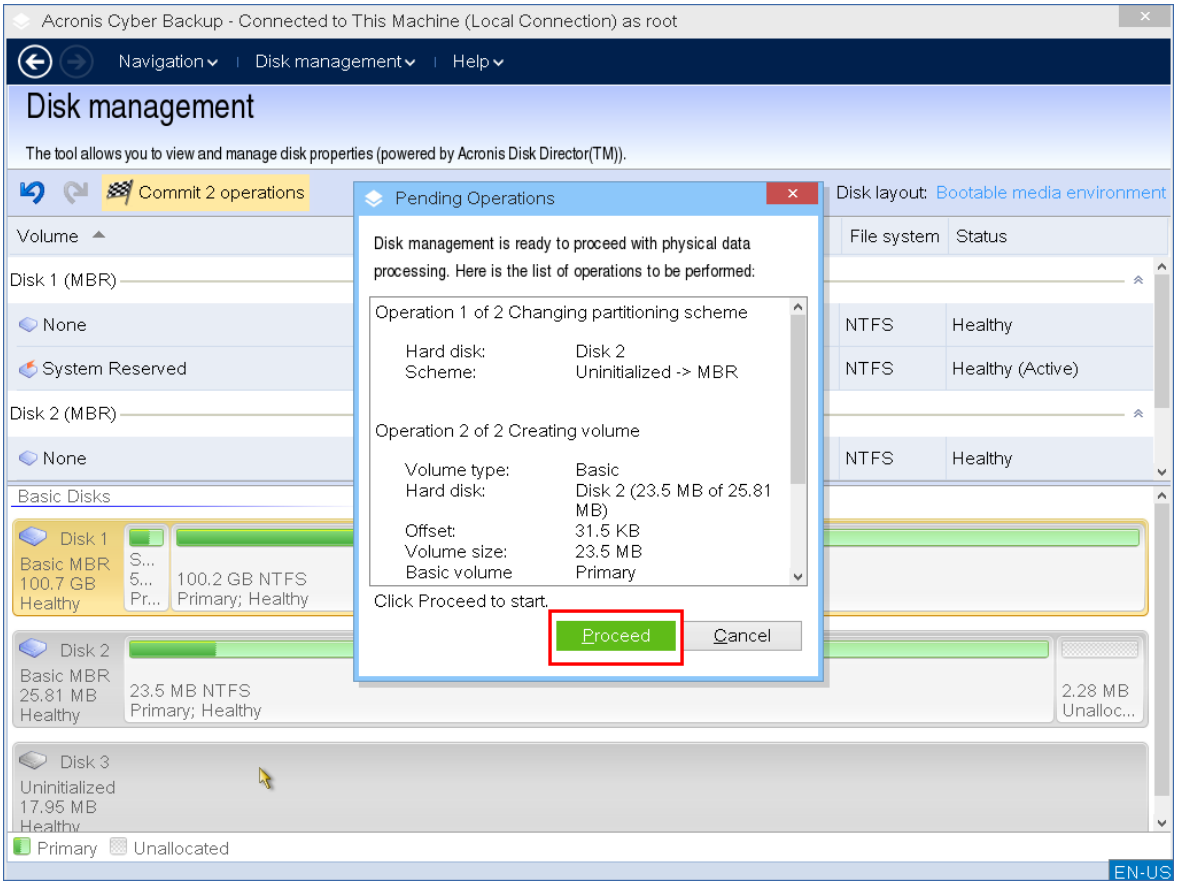
- FAT16 (wyłączony, jeśli ustawiono rozmiar woluminu większy niż 2 GB)
- FAT32 (wyłączony, jeśli ustawiono rozmiar woluminu większy niż 2 TB)
- NTFS
- Pozostaw wolumin niesformatowany.

Ustawiając rozmiar klastra, można wybrać dowolną liczbę spośród wstępnie ustawionych wartości dla każdego systemu plików. Domyślnie proponowany rozmiar klastra jest najlepiej dopasowany do woluminu z wybranym systemem plików. W przypadku ustawienia rozmiaru klastra 64 KB w systemie FAT16/FAT32 lub 8–64 KB w systemie NTFS system Windows będzie mógł zamontować wolumin, ale niektóre programy (na przykład programy instalacyjne) mogą niepoprawnie obliczać miejsce na dysku.

Jeśli tworzysz wolumin standardowy, który może być woluminem systemowym, możesz też wybrać typ woluminu: **Podstawowy** (**Aktywny podstawowy**) lub **Logiczny**. Zazwyczaj wartość **Podstawowy** jest wybierana w celu zainstalowania na woluminie systemu operacyjnego. Wartość **Aktywny** (domyślna) należy wybrać, aby zainstalować na tym woluminie system operacyjny, który będzie uruchamiany podczas rozruchu komputera. W przypadku niewybrania przycisku **Podstawowy** opcja **Aktywny** będzie nieaktywna. Jeśli wolumin ma służyć do magazynowania danych, wybierz **Logiczny**.

Uwaga
Dysk standardowy może zawierać maksymalnie cztery woluminy podstawowe. Jeśli woluminy już istnieją, dysk trzeba przekonwertować na dynamiczny, w przeciwnym razie opcje **Aktywny** i **Podstawowy** będą wyłączone i będzie można wybrać jedynie typ woluminu **Logiczny**.

6. Kliknij **Wykonaj**, a następnie kliknij **Kontynuuj** w oknie **Operacje oczekujące**. Wyjście z programu bez wykonania operacji spowoduje jej skuteczne anulowanie.



Usuwanie woluminu

Aby usunąć wolumin

1. Kliknij prawym przyciskiem myszy wolumin, który chcesz usunąć.
2. Kliknij **Usuń wolumin**.

Uwaga
Wszystkie informacje dostępne na tym woluminie zostaną nieodwracalnie utracone.

3. Kliknięcie przycisku **OK** spowoduje dodanie oczekującej operacji usunięcia woluminu.
4. Aby ukończyć dodaną operację, wykonaj ją. Wyjście z programu bez wykonania operacji spowoduje jej skuteczne anulowanie.

Po usunięciu woluminu dostępne na nim miejsce jest dodawane do nieprzydzielonego miejsca na dysku. Można go użyć w celu utworzenia nowego woluminu lub zmienienia typu innego woluminu.

Ustawianie aktywnego woluminu

Jeśli istnieje kilka woluminów podstawowych, należy wskazać jeden z nich jako wolumin startowy. W tym celu żądany wolumin można ustawić jako aktywny. Na dysku może się znajdować tylko jeden wolumin aktywny.

Aby ustawić wolumin jako aktywny:

1. Kliknij żądany wolumin podstawowy na standardowym dysku MBR, a następnie kliknij **Oznacz jako aktywny**.
   Jeśli w systemie nie ma innego woluminu aktywnego, zostanie dodana oczekująca operacja ustawiania woluminu aktywnego. Jeśli w systemie znajduje się inny wolumin aktywny, najpierw pojawi się ostrzeżenie, że poprzedni wolumin aktywny trzeba ustawić jako pasywny.

   Uwaga
   W wyniku ustawienia nowego woluminu aktywnego litera poprzedniego woluminu aktywnego może ulec zmianie, co może uniemożliwić uruchamianie niektórych zainstalowanych programów.

2. Kliknięcie przycisku **OK** spowoduje dodanie oczekującej operacji ustawiania woluminu aktywnego.

   Uwaga
   Nawet jeśli na nowym woluminie aktywnym znajduje się system operacyjny, w niektórych przypadkach nie można przy jego użyciu uruchomić komputera. Należy potwierdzić decyzję o ustawieniu nowego woluminu jako aktywnego.

3. Aby ukończyć dodaną operację, wykonaj ją. Wyjście z programu bez wykonania operacji spowoduje jej skuteczne anulowanie.

Zmiana litery woluminu

Systemy operacyjne Windows podczas uruchamiania przypisują litery do woluminów dysku twardego (C:, D: itd.). Za pomocą tych liter aplikacje i systemy operacyjne znajdują pliki oraz foldery w woluminach. Podłączenie dodatkowego dysku, a także utworzenie lub usunięcie woluminu na istniejących dyskach, może spowodować zmianę konfiguracji systemu. W rezultacie niektóre aplikacje mogą przestać działać prawidłowo, a automatyczne znajdowanie i otwieranie plików użytkownika może się okazać niemożliwe. Aby temu zapobiec, można ręcznie zmienić litery, które zostały automatycznie przypisane do woluminów przez system operacyjny.

Aby zmienić literę przypisaną do woluminu przez system operacyjny:

1. Kliknij prawym przyciskiem myszy żądany wolumin i kliknij **Zmień literę**.
2. W oknie **Zmień literę** wybierz nową literę.

3. Kliknięcie przycisku **OK** spowoduje dodanie oczekującej operacji przypisywania liter do woluminów.
4. Aby ukończyć dodaną operację, wykonaj ją. Wyjście z programu bez wykonania operacji spowoduje jej skuteczne anulowanie.

Zmiana etykiety woluminu

Etykieta woluminu to atrybut opcjonalny. Jest to nazwa przypisana do woluminu, która ułatwia jego rozpoznawanie.

Aby zmienić etykietę woluminu

1. Kliknij prawym przyciskiem myszy żądany wolumin i kliknij **Zmień etykietę**.
2. Wprowadź nową etykietę w polu tekstowym okna **Zmień etykietę**.
3. Kliknięcie przycisku **OK** spowoduje dodanie oczekującej operacji zmiany etykiety woluminu.
4. Aby ukończyć dodaną operację, wykonaj ją. Wyjście z programu bez wykonania operacji spowoduje jej skuteczne anulowanie.

Formatowanie woluminu

Wolumin można sformatować, aby zmienić jego system plików:

- W celu zaoszczędzenia dodatkowego miejsca, traconego z powodu rozmiaru klastra w systemach plików FAT16 i FAT32.
- W celu szybkiego i stosunkowo skutecznego zniszczenia danych znajdujących się na tym woluminie.

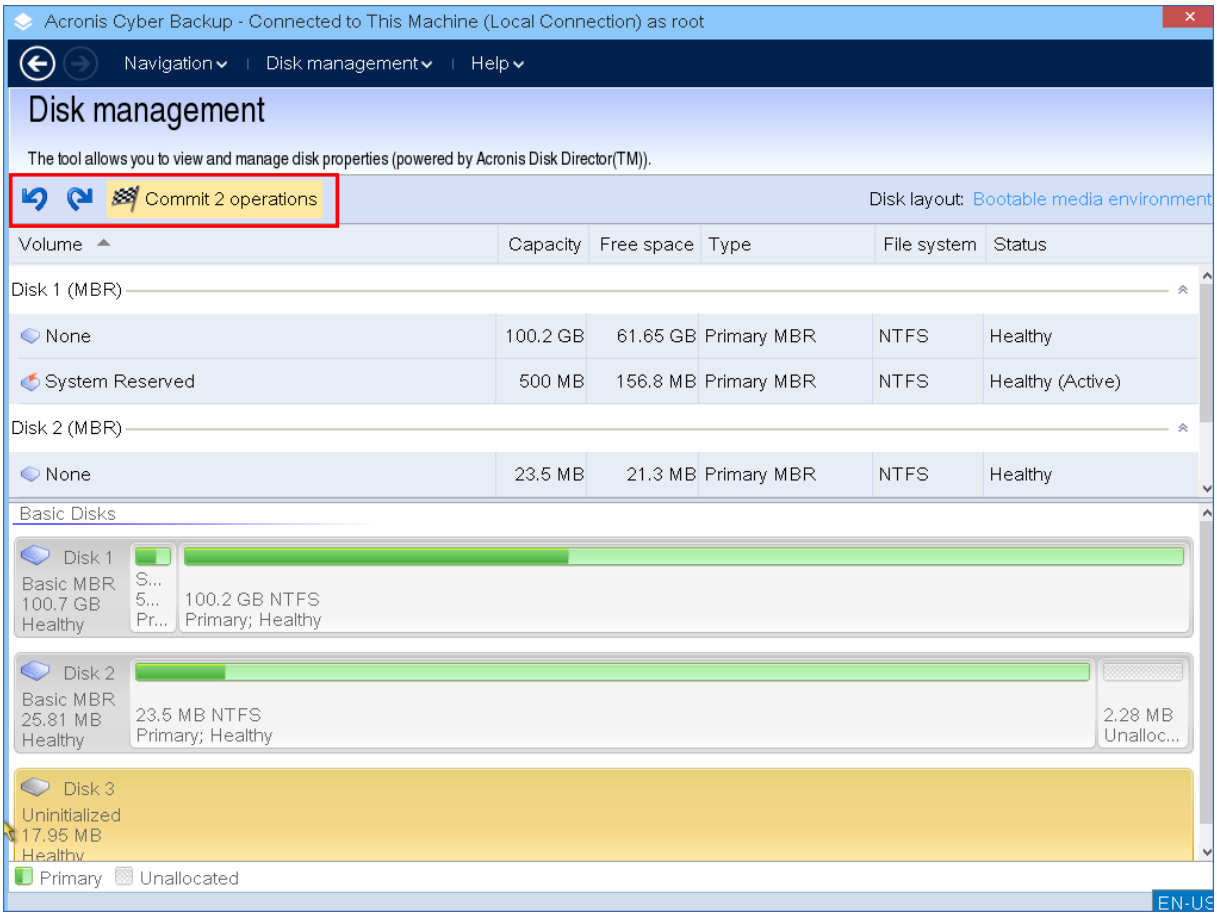
Aby sformatować wolumin:

1. Kliknij prawym przyciskiem myszy żądany wolumin i kliknij **Formatuj**.
2. Wybierz rozmiar klastra i system plików. Możliwe opcje systemu plików to:
   - FAT16 (wyłączony, jeśli ustawiono rozmiar woluminu większy niż 2 GB)
   - FAT32 (wyłączony, jeśli ustawiono rozmiar woluminu większy niż 2 TB)
   - NTFS
3. Kliknięcie przycisku **OK** spowoduje dodanie oczekującej operacji formatowania woluminu.
4. Aby ukończyć dodaną operację, wykonaj ją. Wyjście z programu bez wykonania operacji spowoduje jej skuteczne anulowanie.

Operacje oczekujące

Wszystkie operacje są uznawane za oczekujące, dopóki nie uruchomisz i potwierdzisz polecenia **Wykonaj**. Dzięki temu można kontrolować wszystkie zaplanowane operacje, dokładnie sprawdzać planowane zmiany i w razie potrzeby anulować każdą operację, zanim zostanie wykonana.

Widok **Zarządzanie dyskami** obejmuje pasek narzędzi z ikonami umożliwiającymi wykonywanie określonych działań w odniesieniu do oczekujących operacji: **Cofnij**, **Wykonaj ponownie** i **Wykonaj**. Działania te można też uruchamiać w menu **Zarządzanie dyskami**.



Wszystkie zaplanowane operacje są dodawane do listy operacji oczekujących.

Działanie **Cofnij** umożliwia cofnięcie ostatniej operacji na liście. Jest ono dostępne, jeśli lista nie jest pusta.

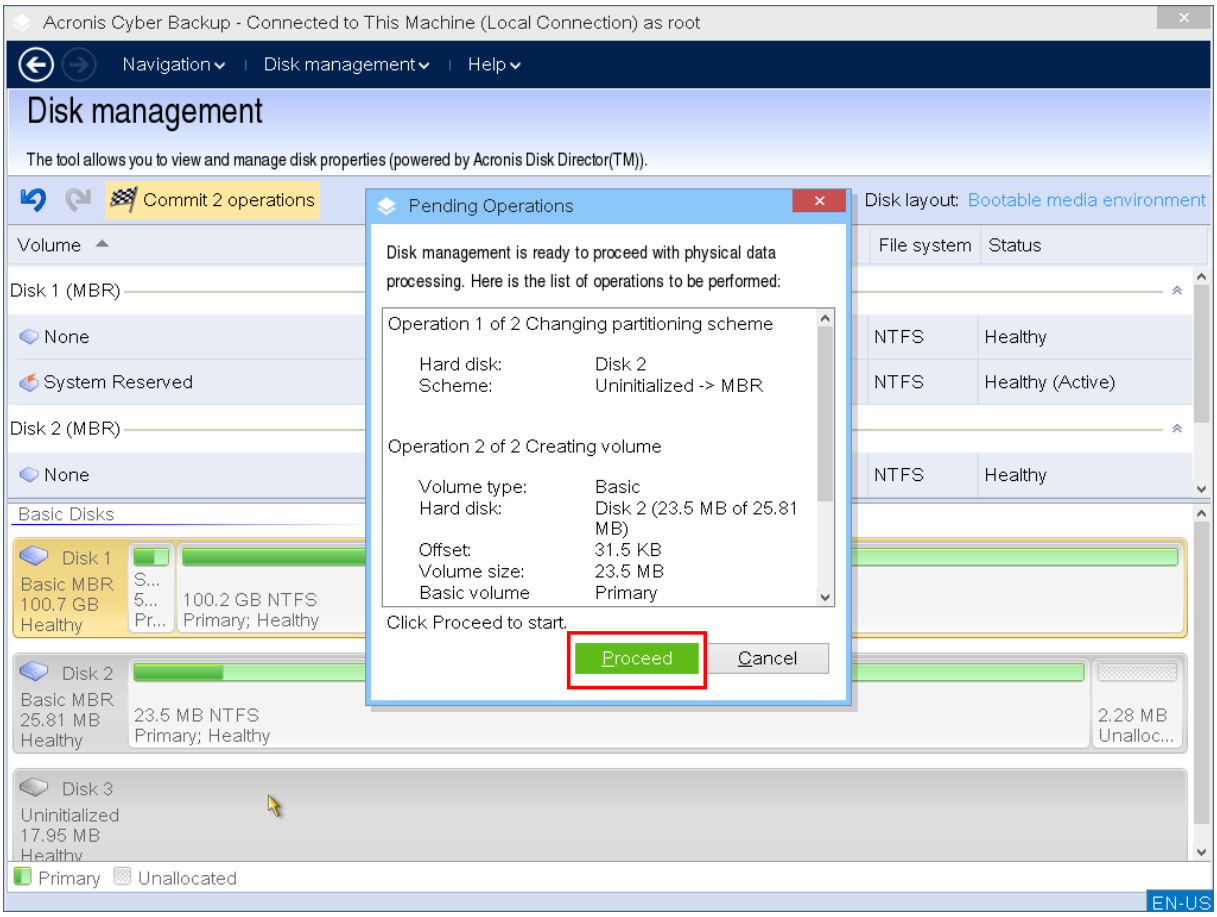
Działanie **Wykonaj ponownie** umożliwia przywrócenie ostatniej operacji oczekującej, która została cofnięta.

Działanie **Wykonaj** powoduje otwarcie okna **Operacje oczekujące**, w którym można przejrzeć listę tych operacji.

Kliknięcie **Kontynuuj** spowoduje ich wykonanie.

Uwaga
Po wybraniu operacji **Kontynuuj** nie można cofnąć żadnych działań ani operacji.

Ponadto klikając **Anuluj** , można anulować wykonanie operacji. Dzięki temu na liście operacji oczekujących nie zostaną wprowadzone żadne zmiany. Wyjście z programu bez wykonania operacji oczekujących również spowoduje ich skuteczne anulowanie.



Operacje zdalne dotyczące nośnika startowego

Aby nośnik startowy był widoczny w konsoli Cyber Protect, trzeba najpierw go zarejestrować zgodnie z opisem podanym w sekcji "Rejestrowanie nośnika na serwerze zarządzania" (s. 400).

Po zarejestrowaniu nośnika w konsoli Cyber Protect będzie on widoczny w obszarze **Urządzenia** > **Nośnik startowy**.

Korzystając z interfejsu internetowego, można zarządzać nośnikiem zdalnie. Można na przykład odzyskać dane, uruchomić ponownie komputer uruchomiony przy użyciu nośnika lub zamknąć system takiego komputera, a także wyświetlić informacje, działania i alerty dotyczące nośnika.

Aby zdalnie odzyskać pliki lub foldery przy użyciu nośnika startowego

1. W konsoli Cyber Protect przejdź do sekcji **Urządzenia** > **Nośnik startowy**.
1. Wybierz nośnik, którego chcesz użyć w celu odzyskania danych.
2. Kliknij **Odzyskiwanie**.
3. Wybierz lokalizację, a następnie potrzebną kopię zapasową. Należy pamiętać, że kopie zapasowe są filtrowane według lokalizacji.
4. Wybierz punkt odzyskiwania, a następnie kliknij **Odzyskaj pliki/foldery**.

5. Przejdź do odpowiedniego folderu lub użyj paska wyszukiwania, aby uzyskać listę wymaganych plików i folderów.

   Można użyć jednego lub kilku symboli wieloznacznych (* i ?). Więcej informacji na temat stosowania symboli wieloznacznych można znaleźć w sekcji "Filtry plików" (s. 284).
6. Kliknij, aby wybrać pliki, które chcesz odzyskać, a następnie kliknij **Odzyskaj**.
7. W polu **Ścieżka** wybierz miejsce docelowe odzyskiwania.
8. [Opcjonalnie] Aby przeprowadzić zaawansowaną konfigurację odzyskiwania, kliknij **Opcje odzyskiwania**. Więcej informacji można znaleźć w sekcji "Opcje odzyskiwania" (s. 344).
9. Kliknij **Rozpocznij odzyskiwanie**.
10. Wybierz jedną z następujących opcji zastępowania plików:
    - **Zastąp istniejące pliki**
    - **Zastąp istniejący plik, jeśli jest starszy**
    - **Nie zastępuj istniejących plików**

    Określ, czy komputer ma zostać automatycznie ponownie uruchomiony.
11. Kliknij **Kontynuuj**, aby rozpocząć odzyskiwanie. Na karcie **Działania** jest wyświetlany postęp odzyskiwania.

Aby zdalnie odzyskać dyski, woluminy lub całe komputery przy użyciu nośnika startowego

1. Na karcie **Urządzenia** przejdź do grupy **Nośnik startowy**, a następnie wybierz nośnik, którego chcesz użyć w celu odzyskania danych.
2. Kliknij **Odzyskiwanie**.
3. Wybierz lokalizację, a następnie potrzebną kopię zapasową. Należy pamiętać, że kopie zapasowe są filtrowane według lokalizacji.
4. Wybierz punkt odzyskiwania, a następnie kliknij **Odzyskaj** > **Cały komputer**.

   W razie potrzeby skonfiguruj komputer docelowy i mapowanie woluminów zgodnie z opisem podanym w sekcji "Odzyskiwanie komputera fizycznego" (s. 324).
5. Aby przeprowadzić zaawansowaną konfigurację odzyskiwania, kliknij **Opcje odzyskiwania**. Więcej informacji można znaleźć w sekcji "Opcje odzyskiwania" (s. 344).
6. Kliknij **Rozpocznij odzyskiwanie**.
7. Potwierdź, że chcesz zastąpić dyski ich wersjami z kopii zapasowej. Określ, czy komputer ma zostać automatycznie ponownie uruchomiony.
8. Na karcie **Działania** jest wyświetlany postęp odzyskiwania.

Aby zdalnie uruchomić ponownie komputer uruchomiony przy użyciu nośnika

1. Na karcie **Urządzenia** przejdź do grupy **Nośnik startowy**, a następnie wybierz nośnik, którego chcesz użyć w celu odzyskania danych.
2. Kliknij **Uruchom ponownie**.
3. Potwierdź, że chcesz uruchomić ponownie komputer uruchomiony przy użyciu nośnika.

Aby zdalnie zamknąć system komputera uruchomionego przy użyciu nośnika

1. Na karcie **Urządzenia** przejdź do grupy **Nośnik startowy**, a następnie wybierz nośnik, którego chcesz użyć w celu odzyskania danych.
2. Kliknij **Zamknij system**.
3. Potwierdź, że chcesz zamknąć system komputera uruchomionego przy użyciu nośnika.

Aby wyświetlić informacje o nośniku startowym

1. Na karcie **Urządzenia** przejdź do grupy **Nośnik startowy**, a następnie wybierz nośnik, którego chcesz użyć w celu odzyskania danych.
2. Kliknij **Szczegóły**, **Działania** lub **Alerty**, aby wyświetlić odpowiednie informacje.

Aby zdalnie usunąć nośnik startowy

1. Na karcie **Urządzenia** przejdź do grupy **Nośnik startowy**, a następnie wybierz nośnik, którego chcesz użyć w celu odzyskania danych.
2. Kliknij **Usuń**, aby usunąć nośnik startowy z konsoli Cyber Protect.
3. Potwierdź, że chcesz usunąć nośnik startowy.

Konfigurowanie urządzeń iSCSI

W tej sekcji opisano konfigurowanie urządzeń Internet Small Computer System Interface (iSCSI) podczas pracy z nośnikiem startowym. Po wykonaniu poniższych czynności będzie można używać tych urządzeń tak, jakby były podłączone lokalnie do komputera uruchomionego za pomocą nośnika startowego.

Serwer obiektu docelowego iSCSI (lub **portal docelowy**) to serwer, który służy jako host urządzenia iSCSI. **Obiekt docelowy iSCSI** to komponent docelowego serwera, przy czym ten komponent udostępnia urządzenie i zawiera listę inicjatorów iSCSI, które mogą uzyskać dostęp do urządzenia. **Inicjator iSCSI** to komponent komputera, przy czym ten komponent zapewnia interakcję między komputerem i obiektem docelowym iSCSI. W przypadku konfigurowania dostępu do urządzenia iSCSI na komputerze uruchomionym za pomocą nośnika startowego musisz określić portal obiektu docelowego iSCSI urządzenia i jeden z inicjatorów iSCSI określonych w obiekcie docelowym. Jeśli obiekt docelowy współużytkuje kilka urządzeń, uzyskasz dostęp do każdego z nich.

Aby dodać urządzenie iSCSI na nośniku startowym opartym na systemie Linux

1. Kliknij **Narzędzia** > **Skonfiguruj urządzenia iSCSI/NDAS**.
2. Kliknij **Dodaj hosta**.
3. Określ adres IP i port docelowego portalu iSCSI oraz nazwę dowolnego inicjatora iSCSI, który może uzyskać dostęp do urządzenia.
4. Jeśli host wymaga uwierzytelniania, określ odpowiednią nazwę użytkownika i hasło.
5. Kliknij **OK**.
6. Wybierz obiekt docelowy iSCSI z listy, a następnie kliknij **Połącz**.

7. Jeśli w ustawieniach obiektu docelowego iSCSI jest włączone uwierzytelnianie CHAP, pojawi się monit o podanie poświadczeń w celu uzyskania dostępu do tego obiektu. Podaj tę samą nazwę użytkownika i klucz tajny obiektu docelowego iSCSI, które określono w ustawieniach tego obiektu. Kliknij **OK**.
8. Kliknij **Zamknij**, aby zamknąć okno.

Aby dodać urządzenie iSCSI na nośniku startowym opartym na środowisku PE

1. Kliknij kolejno **Narzędzia** > **Uruchom instalację iSCSI**.
2. Kliknij kartę **Wykrywanie**.
3. W obszarze **Portale docelowe** kliknij **Dodaj**, a następnie określ adres IP i port docelowego portalu iSCSI. Kliknij **OK**.
4. Kliknij kartę **Ogólne**, kliknij **Zmień**, a następnie określ nazwę dowolnego inicjatora iSCSI, który może uzyskać dostęp do urządzenia.
5. Kliknij kartę **Miejsca docelowe**, kliknij **Odśwież**, wybierz obiekt docelowy iSCSI z listy, a następnie kliknij **Połącz**. Kliknij **OK**, aby nawiązać połączenie z obiektem docelowym iSCSI.
6. Jeśli w ustawieniach obiektu docelowego iSCSI jest włączone uwierzytelnianie CHAP, pojawi się komunikat o błędzie **Niepowodzenie uwierzytelnienia**. W takim przypadku kliknij **Połącz**, kliknij **Zaawansowane**, zaznacz pole wyboru **Włącz logowanie CHAP** i podaj tę samą nazwę użytkownika i klucz tajny obiektu docelowego iSCSI, które określono w ustawieniach tego obiektu. Kliknij **OK**, aby zamknąć okno, a następnie kliknij **OK**, aby nawiązać połączenie z obiektem docelowym iSCSI.
7. Kliknij **OK**, aby zamknąć okno.

Startup Recovery Manager

Startup Recovery Manager to komponent startowy, który znajduje się na dysku twardym. Za pomocą narzędzia Startup Recovery Manager można uruchomić ratunkowe narzędzie startowe bez użycia osobnego nośnika startowego.

Startup Recovery Manager szczególnie przydaje się użytkownikom podróżującym. W razie niepowodzenia operacji uruchom ponownie komputer, poczekaj na wyświetlenie monitu „Naciśnij klawisz F11, aby uruchomić program **Acronis Startup Recovery Manager**", a następnie naciśnij klawisz F11. Program zostanie uruchomiony i będzie można przeprowadzić odzyskiwanie. W przypadku komputerów z zainstalowanym programem ładującym GRUB podczas ponownego uruchamiania systemu wybierz z menu startowego program Startup Recovery Manager i nie naciskaj klawisza F11.

Ponadto podczas podróży można używać programu Startup Recovery Manager do tworzenia kopii zapasowych.

Aby skorzystać z narzędzia Startup Recovery Manager, trzeba je aktywować. Spowoduje to włączenie monitu startowego **Naciśnij klawisz F11, aby uruchomić program Acronis Startup Recovery Manager** (lub dodaj pozycję **Startup Recovery Manager** do menu programu ładującego GRUB, jeśli z niego korzystasz).

Uwaga
W celu aktywacji programu Startup Recovery Manager na komputerze z niezaszyfrowanym woluminem systemowym na tym komputerze musi być co najmniej 100 MB wolnego miejsca. W przypadku operacji odzyskiwania, które wymagają ponownego uruchomienia komputera, potrzeba kolejnych 100 MB.

Możesz aktywować narzędzie Startup Recovery Manager na komputerze z woluminem zaszyfrowanym przy użyciu funkcji BitLocker, jeżeli komputer ten ma przynajmniej jeden inny wolumin, który nie jest zaszyfrowany. Na tym woluminie niezaszyfrowanym musi się znajdować co najmniej 500 MB wolnego miejsca. W przypadku operacji odzyskiwania, które wymagają ponownego uruchomienia komputera, wymagane jest dodatkowe 500 MB wolnego miejsca.

Ważne
Jeżeli aktywowanie narzędzia Startup Recovery Manager będzie niemożliwe, to operacje tworzenia kopii zapasowych na potrzeby funkcji Odzyskiwanie jednym kliknięciem zakończą się niepowodzeniem.

Jeśli nie jest używany program ładujący GRUB zainstalowany w głównym rekordzie startowym (MBR), program Startup Recovery Manager podczas aktywacji zastępuje rekord MBR własnym kodem startowym. W związku z tym może być konieczna ponowna aktywacja programów ładujących innych producentów, jeśli takie programy są zainstalowane.

Jeśli w systemie Linux jest używany inny program ładujący niż GRUB (na przykład LILO), warto przed aktywacją narzędzia Startup Recovery Manager zainstalować program ładujący w rekordzie rozruchowym partycji root (lub boot) systemu Linux, a nie w głównym rekordzie rozruchowym. W przeciwnym razie należy ponownie skonfigurować program ładujący po aktywacji.

Aktywowanie programu Startup Recovery Manager

Na komputerze z uruchomionym agentem dla systemu Windows lub agentem dla systemu Linux program Startup Recovery Manager można aktywować przy użyciu konsoli internetowej Cyber Protect.

Aby aktywować program Startup Recovery Manager w konsoli usługi Cyber Protect

1. Wybierz komputer, na której chcesz aktywować program Startup Recovery Manager.
2. Kliknij opcję **Szczegóły**.
3. Włącz przełącznik **Startup Recovery Manager**.
4. Poczekaj, aż oprogramowanie aktywuje program Startup Recovery Manager.

Aby aktywować program Startup Recovery Manager na komputerze bez zainstalowanego agenta

1. Uruchom komputer za pomocą nośnika startowego.
2. Kliknij **Narzędzia** > **Aktywuj program Startup Recovery Manager**.
3. Poczekaj, aż oprogramowanie aktywuje program Startup Recovery Manager.

Dezaktywowanie programu Startup Recovery Manager

Aby dezaktywować program Startup Recovery Manager, powtórz procedurę aktywacji, ale wybierając odwrotne czynności. Dezaktywacja powoduje wyłączenie monitu startowego **Naciśnij klawisz F11, aby uruchomić program Acronis Startup Recovery Manager** (lub odpowiedniej pozycji menu w programie GRUB).

Jeśli program Startup Recovery Manager jest wyłączony, a system się nie uruchomi, w celu odzyskania systemu należy wykonać jedną z poniższych czynności:

- Uruchomić komputer przy użyciu oddzielnego nośnika startowego
- Użyć funkcji uruchamiania przez sieć z serwera PXE Server lub usług instalacji zdalnej (RIS) firmy Microsoft

Acronis PXE Server

Serwer Acronis PXE Server umożliwia uruchamianie komputerów do komponentów startowych rozwiązań Acronis przez sieć.

Uruchomienie przez sieć:

- eliminuje potrzebę obecności technika w miejscu instalacji nośnika startowego w systemie, który musi zostać uruchomiony;
- w czasie operacji grupowych skraca czas potrzebny do uruchomienia wielu komputerów (w porównaniu z korzystaniem z fizycznego nośnika startowego).

Komponenty startowe są przesyłane na serwer Acronis PXE Server przy użyciu narzędzia Acronis Bootable Media Builder. Aby przesłać komponenty startowe, uruchom generator nośnika startowego, a następnie wykonaj szczegółowe instrukcje opisane w sekcji „Nośnik startowy oparty na systemie Linux”.

Uruchamianie wielu komputerów z serwera Acronis PXE Server ma sens, jeśli w sieci znajduje się serwer DHCP (Dynamic Host Control Protocol). Dzięki niemu interfejsy sieciowe uruchamianych komputerów automatycznie uzyskują adresy IP.

Ograniczenie:

Serwer Acronis PXE Server nie obsługuje programu ładującego UEFI.

Instalowanie serwera Acronis PXE Server

Aby zainstalować serwer Acronis PXE Server

1. Zaloguj się jako administrator i uruchom program instalacyjny produktu Acronis Cyber Protect.
2. [Opcjonalnie] Aby zmienić język programu instalacyjnego, kliknij **Skonfiguruj język**.
3. Zaakceptuj warunki umowy licencyjnej i zasady ochrony prywatności, a następnie kliknij **Kontynuuj**.

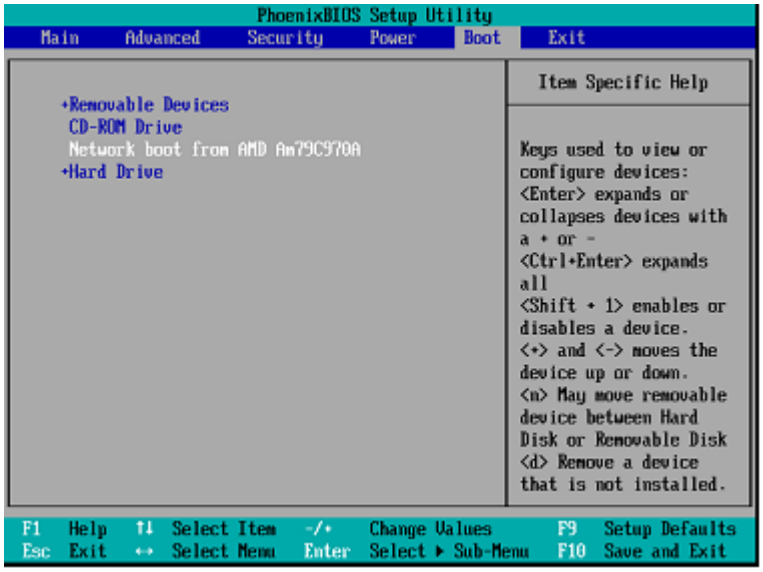
4. Kliknij **Dostosuj ustawienia instalacji**.
5. Obok pozycji **Elementy do zainstalowania** kliknij **Zmień**.
6. Zaznacz pole wyboru **PXE Server**. Jeśli nie chcesz instalować na komputerze innych komponentów, usuń zaznaczenia odpowiednich pól wyboru. Kliknij **Gotowe**, aby kontynuować.
7. [Opcjonalnie] Zmień inne ustawienia instalacji.
8. Kliknij **Zainstaluj**, aby kontynuować instalację.
9. Po zakończeniu instalacji kliknij **Zamknij**.

Serwer Acronis PXE Server jest uruchamiany jako usługa niezwłocznie po zakończeniu procesu instalacji. Później będzie on uruchamiał się automatyczne przy każdym uruchomieniu systemu. Serwer Acronis PXE Server można zatrzymać i uruchomić tak samo jak inne usługi systemu Windows.

Konfigurowanie komputera do uruchamiania z serwera PXE

W przypadku komputera bez systemu operacyjnego wystarczy, aby system BIOS komputera obsługiwał uruchamianie przez sieć.

Na komputerze, na którego dysku twardym znajduje się system operacyjny, system BIOS należy skonfigurować tak, aby karta sieciowa była pierwszym urządzeniem startowym lub przynajmniej urządzeniem poprzedzającym dysk twardy. Poniższy przykład przedstawia jedną z właściwych konfiguracji systemu BIOS. Jeśli do komputera nie zostanie włożony nośnik startowy, komputer uruchomi się z sieci.



W niektórych wersjach systemu BIOS po włączeniu karty interfejsu sieciowego należy zapisać zmiany, aby karta pojawiła się na liście urządzeń startowych.

Jeśli komputer jest wyposażony w wiele kart interfejsu sieciowego, należy się upewnić, że do karty obsługiwanej przez system BIOS jest podłączony kabel sieciowy.

Praca w podsieciach

Aby umożliwić pracę serwera Acronis PXE Server w innej podsieci (przez przełącznik), skonfiguruj przełącznik tak, aby przekazywał ruch serwera PXE. Adresy IP serwera PXE konfiguruje się dla każdego interfejsu przy użyciu funkcji pomocnika IP w taki sam sposób jak adresy serwera DHCP. Aby uzyskać więcej informacji, zobacz: https://docs.microsoft.com/en-us/troubleshoot/mem/configmgr/boot-from-pxe-server.

Ochrona urządzeń mobilnych

Aplikacja do tworzenia kopii zapasowych umożliwia utworzenie kopii zapasowej danych z urządzenia mobilnego w chmurze, a następnie odzyskanie tych danych w razie ich utraty lub uszkodzenia. Uwaga: tworzenie kopii zapasowych w chmurze wymaga konta i subskrypcji chmury Cloud.

Obsługiwane urządzenia mobilne

Aplikację do tworzenia kopii zapasowych można zainstalować na urządzeniu mobilnym z jednym z następujących systemów operacyjnych:

- iOS 10.3 lub nowszy (urządzenia iPhone, iPod i iPad)
- Android 5.0 lub nowszy

Elementy, które można uwzględnić w kopii zapasowej

- Kontakty
- Zdjęcia
- Wideo
- Kalendarze
- Przypomnienia (tylko na urządzeniach z systemem iOS)

Co trzeba wiedzieć

- Kopie zapasowe danych można tworzyć tylko w chmurze.
- Po każdym otwarciu aplikacji pojawi się podsumowanie zmian w danych i będzie można ręcznie rozpocząć tworzenie kopii zapasowej.
- Funkcja **Ciągła kopia zapasowa** jest domyślnie włączona. Jeśli to ustawienie jest włączone:
  - W przypadku systemu Android 7.0 lub nowszego aplikacja do tworzenia kopii zapasowych automatycznie i na bieżąco wykrywa nowe dane oraz przesyła je do środowiska Cloud.
  - W przypadku systemu Android 5 i 6 aplikacja sprawdza zmiany co 3 godziny. Opcję ciągłej kopii zapasowej można wyłączyć w ustawieniach aplikacji.
- Opcja **Używaj tylko połączenia Wi-Fi** jest domyślnie włączona w ustawieniach aplikacji. Jeśli to ustawienie jest włączone, aplikacja do tworzenia kopii zapasowych będzie tworzyć kopię zapasową danych tylko wtedy, gdy będzie dostępne połączenie Wi-Fi. W przypadku braku połączenia Wi-Fi tworzenie kopii zapasowej nie zostanie rozpoczęte. Jeśli aplikacja ma korzystać również z połączenia przez sieć telefonii komórkowej, wyłącz tę opcję.
- Można oszczędzać energię na dwa sposoby:
  - Przy użyciu funkcji **Twórz kopię podczas ładowania**, która jest domyślnie wyłączona. Jeśli to ustawienie jest włączone, aplikacja do tworzenia kopii zapasowych będzie tworzyć kopię

zapasową danych tylko wtedy, gdy urządzenie jest podłączone do źródła zasilania. W przypadku odłączenia urządzenia od źródła zasilania podczas tworzenia ciągłej kopii zapasowej operacja ta zostanie wstrzymana.

  - Przy użyciu opcji **Tryb energooszczędny**, która jest domyślnie włączona. Jeśli to ustawienie jest włączone, aplikacja do tworzenia kopii zapasowych będzie tworzyć kopię zapasową danych tylko wtedy, gdy stan naładowania baterii nie jest niski. Gdy stan naładowania baterii będzie niski, tworzenie ciągłej kopii zapasowej zostanie wstrzymane. Ta opcja jest dostępna w przypadku systemu Android w wersji 8 lub nowszej.

- 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 dowolne urządzenie za pomocą konsoli internetowej Cyber Protect.
- 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 tylko najnowszą wersję danych. Jeśli potrzebujesz odzyskać dane z określonej wersji kopii zapasowej, skorzystaj z konsoli internetowej Cyber Protect na tablecie lub komputerze.
- [Tylko w przypadku urządzeń z systemem Android] 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 do folderu **Odzyskano przy użyciu kopii zapasowej** na karcie SD, jeśli jest ona dostępna podczas odzyskiwania, lub aplikacja wyświetli monit o wskazanie innej lokalizacji, do której mają zostać odzyskane dane.

Jak uzyskać aplikację do tworzenia kopii zapasowych

1. Na urządzeniu mobilnym otwórz przeglądarkę i przejdź do strony https://backup.acronis.com/.
2. Zaloguj się przy użyciu swojego konta.
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.

Jak rozpocząć tworzenie kopii zapasowej danych

1. Otwórz aplikację.
2. Zaloguj się przy użyciu swojego konta.

Stuknij **Skonfiguruj**, aby utworzyć pierwszą kopię zapasową.

1. Wybierz kategorie danych, które chcesz uwzględnić w kopii zapasowej. Domyślnie wybrane są wszystkie kategorie.
2. [Opcjonalnie] Włącz opcję **Szyfruj kopię zapasową**, aby chronić kopię zapasową przez jej zaszyfrowanie. W takim przypadku trzeba będzie również:
   a. Dwa razy wprowadzić hasło szyfrowania.

      Uwaga
      Dobrze zapamiętać hasło, ponieważ zapomnianego hasła nie da się przywrócić ani zmienić.

   b. Stuknij **Szyfruj**.
3. Stuknij **Utwórz kopię zapasową**.
4. 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.

Jak odzyskać dane na urządzenie mobilne

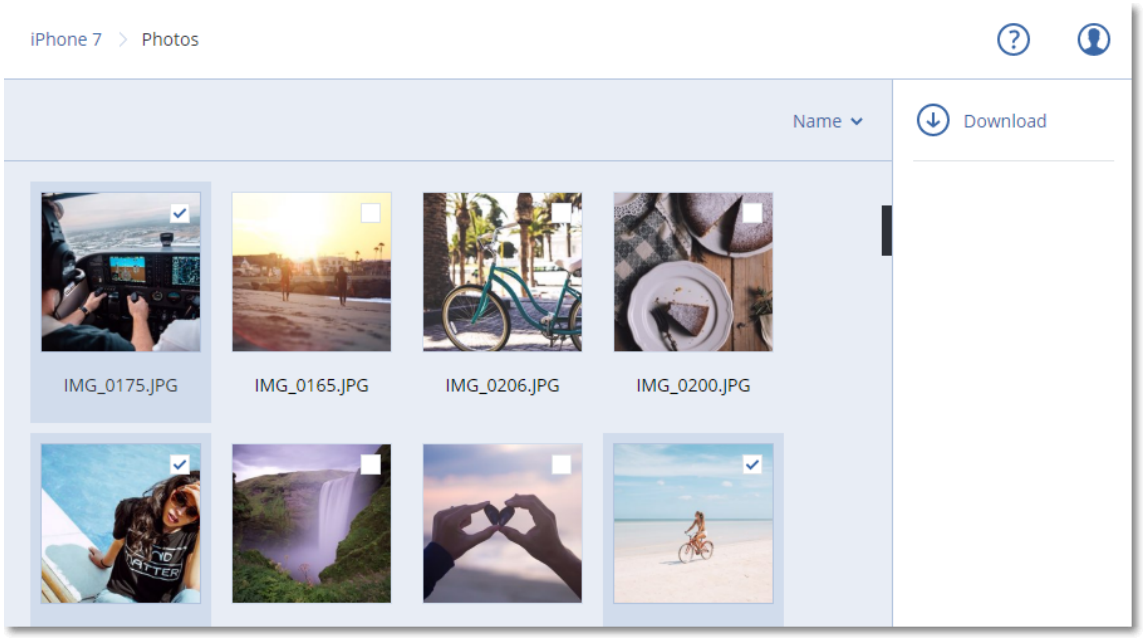
1. Otwórz aplikację do tworzenia kopii zapasowych.
2. Stuknij **Przeglądaj**.
3. Stuknij nazwę urządzenia.
4. Wykonaj jedną z następujących czynności:
   - Aby odzyskać wszystkie dane z kopii zapasowej, stuknij **Odzyskaj wszystko**. Nie trzeba wykonywać żadnych innych czynności.
   - Aby odzyskać tylko wybrane kategorie danych, stuknij **Wybierz**, a następnie stuknij pola wyboru wymaganych kategorii danych. Stuknij **Odzyskaj**. Nie trzeba wykonywać żadnych innych czynności.
   - 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**.

Jak przeglądać dane za pomocą konsoli internetowej Cyber Protect

1. Na komputerze otwórz przeglądarkę i wpisz adres URL konsoli internetowej Cyber Protect.
2. Zaloguj się przy użyciu swojego konta.

3. W obszarze **Wszystkie urządzenia** kliknij **Odzyskaj** pod nazwą urządzenia mobilnego.
4. Wykonaj dowolne z następujących czynności:
   - Aby pobrać wszystkie zdjęcia, filmy, kontakty, kalendarze lub przypomnienia, wybierz odpowiednią kategorię danych. Kliknij **Pobierz**.

   - Aby pobrać wybrane zdjęcia, filmy, kontakty, kalendarze lub przypomnienia, kliknij nazwę odpowiedniej kategorii danych, a następnie zaznacz pola wyboru obok potrzebnych elementów danych. Kliknij **Pobierz**.



   - Aby wyświetlić zdjęcie lub kontakt, kliknij nazwę odpowiedniej kategorii danych, a następnie kliknij wymagany element danych.

Ochrona aplikacji firmy Microsoft

Ważne
Niektóre funkcje opisane w tej sekcji są dostępne tylko w przypadku wdrożeń lokalnych.

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 ochrony do odzyskiwania po awarii oraz ochrony danych.

W przypadku programu Microsoft Exchange Server możesz wybrać **kopię zapasową skrzynki pocztowej**. Jest to kopia zapasowa indywidualnych skrzynek pocztowych za pośrednictwem protokołu Exchange Web Services. Skrzynki pocztowe lub elementy skrzynek pocztowych można odzyskać na aktywny serwer Exchange Server lub do usługi Microsoft 365. Kopia zapasowa skrzynki pocztowej jest obsługiwana w przypadku programu Microsoft Exchange Server 2010 z dodatkiem Service Pack 1 (SP1) lub nowszego.

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 Bazy danych jako pliki	Cały komputer Bazy danych do działającej instancji serwera SQL Bazy danych jako pliki	Cały komputer
Microsoft Exchange Server	Bazy danych do działającego programu Exchange Bazy danych jako pliki Odzyskiwanie granularne na aktywny serwer programu Exchange lub do usługi Microsoft 365*	Cały komputer Bazy danych do działającego programu Exchange Bazy danych jako pliki Odzyskiwanie granularne na aktywny serwer programu Exchange lub do usługi Microsoft 365*	Cały komputer
Serwery baz danych programu Microsoft SharePoint	Bazy danych do działającej instancji serwera SQL Bazy danych jako pliki Odzyskiwanie granularne przy użyciu programu SharePoint Explorer	Cały komputer Bazy danych do działającej instancji serwera SQL Bazy danych jako pliki Odzyskiwanie granularne przy użyciu programu SharePoint Explorer	Cały komputer
Internetowe serwery frontonu programu Microsoft	-	-	Cały komputer

SharePoint			
Usługi domenowe Active Directory	-	Cały komputer	-

* Odzyskiwanie granularne jest również dostępne dla kopii zapasowych skrzynek pocztowych.

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.
- 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.

  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.

Uwaga
Agent dla programu Exchange potrzebuje do działania tymczasowego magazynu. Domyślnie pliki tymczasowe są umieszczane w folderze `%ProgramData%\Acronis\Temp`. Ilość wolnego miejsca na woluminie, na którym znajduje się folder `%ProgramData%`, musi wynosić co najmniej 15 procent rozmiaru bazy danych programu Exchange. Przed rozpoczęciem tworzenia kopii zapasowych programu Exchange można zmienić lokalizację plików tymczasowych, postępując zgodnie z opisem podanym w artykule https://kb.acronis.com/content/40040.

Na kontrolerze domeny upewnij się, że:

- Jest włączony moduł zapisujący Active Directory dla usługi VSS.

Tworząc plan ochrony, upewnij się, że:

- W przypadku komputerów fizycznych jest włączona opcja tworzenia kopii zapasowych Usługa kopiowania woluminów w tle (VSS).
- W przypadku maszyn wirtualnych jest włączona opcja tworzenia kopii zapasowych Usługa kopiowania woluminów w tle (VSS) dla maszyn wirtualnych.

Dodatkowe wymagania dotyczące kopii zapasowych uwzględniających aplikacje

Podczas tworzenia planu ochrony dopilnuj, aby dla kopii zapasowej została wybrana opcja **Cały komputer**. W planie ochrony musi być wyłączona opcja tworzenia kopii zapasowych **Sektor po sektorze**. W przeciwnym razie nie będzie można odzyskać danych aplikacji z kopii zapasowych utworzonych w tym trybie. Odzyskanie danych aplikacji nie będzie możliwe również w przypadku wykonania planu w trybie **Sektor po sektorze** w wyniku automatycznego włączenia tego trybu.

Wymagania dotyczące maszyn wirtualnych ESXi

Jeśli aplikacja działa na maszynie wirtualnej, której kopie zapasowe tworzy agent dla VMware, upewnij się, że:

- Maszyna wirtualna uwzględniana w kopii zapasowej spełnia wymagania wyciszenia spójnego z aplikacjami wymienione w artykule „Windows Backup Implementations" (Implementacje funkcji kopii zapasowych systemu Windows) w dokumentacji rozwiązania VMware: https://code.vmware.com/docs/1674/virtual-disk-programming-guide/doc/vddkBkupVadp.9.6.html.
- Na maszynie są zainstalowane aktualne narzędzia VMware Tools.
- Na maszynie 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).

Wymagania dotyczące maszyn wirtualnych Hyper-V

Jeśli aplikacja działa na maszynie wirtualnej, której kopie zapasowe tworzy agent dla Hyper-V, upewnij się, że:

- System operacyjny-gość to Windows Server 2008 lub nowszy.
- W przypadku programu Hyper-V 2008 R2: system operacyjny-gość to Windows Server 2008/2008 R2/2012.
- Maszyna wirtualna nie ma żadnych dysków dynamicznych.
- Między hostem Hyper-V a systemem operacyjnym-gościem istnieje połączenie sieciowe. Jest ono niezbędne do wykonywania zdalnych zapytań WMI wewnątrz maszyny wirtualnej.

- Na maszynie 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).
- Konfiguracja maszyny wirtualnej spełnia następujące kryteria:
  - Są zainstalowane i aktualne Usługi integracji funkcji Hyper-V. Aktualizacja krytyczna to https://support.microsoft.com/en-us/help/3063109/hyper-v-integration-components-update-for-windows-virtual-machines
  - W ustawieniach maszyny wirtualnej jest włączona opcja **Zarządzanie** > **Usługi integracji** > **Kopia zapasowa (punkt kontrolny woluminu)**.
  - W przypadku programu Hyper-V 2012 lub nowszego: maszyna wirtualna nie ma żadnych punktów kontrolnych.
  - W przypadku programu Hyper-V 2012 R2 lub nowszego: maszyna wirtualna ma kontroler SCSI (sprawdź **Ustawienia** > **Sprzęt**).

Kopia zapasowa bazy danych

Przed utworzeniem kopii zapasowej baz danych dopilnuj, aby zostały spełnione wymagania wymienione w sekcji „Wymagania wstępne”.

Wybierz bazy danych zgodnie z poniższym opisem, a następnie odpowiednio określ inne ustawienia planu ochrony.

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 ochrony.

Aby wybrać bazy danych SQL

1. Kliknij **Urządzenia** > **Microsoft SQL**.
   W oprogramowaniu zostanie pokazane drzewo zawsze włączonych grup dostępności (AAG) programu SQL Server, komputerów z uruchomionym programem Microsoft SQL Server, instancji programu SQL Server i baz danych.
2. Przejdź do danych, które chcesz uwzględnić w kopii zapasowej.
   Rozwiń węzły drzewa lub klikaj dwukrotnie elementy na liście po prawej stronie drzewa.
3. Wybierz dane, które chcesz uwzględnić w kopii zapasowej. Możesz wybrać zawsze włączone grupy dostępności (AAG), komputery z uruchomionym programem SQL Server, instancje programu SQL Server lub poszczególne bazy danych.
   - W przypadku wybrania zawsze włączonej grupy dostępności (AAG) w kopii zapasowej zostaną uwzględnione wszystkie bazy danych należące do wybranej zawsze włączonej grupy

dostępności (AAG). Więcej informacji o tworzeniu kopii zapasowych zawsze włączonych grup dostępności lub pojedynczych baz danych zawsze włączonych grup dostępności można znaleźć w artykule „Ochrona zawsze włączonych grup dostępności”.

- W przypadku wybrania komputera z programem SQL Server zostaną utworzone kopie zapasowe wszystkich baz danych dołączonych do wszystkich instancji serwera SQL na wybranym komputerze.
- W przypadku wybrania instancji serwera SQL zostaną utworzone kopie zapasowe wszystkich baz danych przyłączonych do wybranej instancji.
- W przypadku bezpośredniego wybrania baz danych w kopii zapasowej będą uwzględniane tylko wybrane bazy danych.

4. Kliknij **Chroń**. Jeśli pojawi się monit, podaj poświadczenia umożliwiające dostęp do danych programu SQL Server.

   W przypadku korzystania z funkcji uwierzytelniania dostępnej w systemie Windows konto musi należeć do grupy **Operatorzy kopii zapasowych** lub **Administratorzy** na danym komputerze oraz do roli **administrator systemu** w każdej instancji uwzględnianej w kopii zapasowej.

   W przypadku korzystania z funkcji uwierzytelniania dostępnej w programie SQL Server konto musi należeć do roli **administrator systemu** w każdej instancji uwzględnianej w kopii zapasowej.

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**
2010/2013/2016/2019	Bazy danych, grupy dostępności bazy danych	Członkostwo w grupie z rolą **Zarządzanie serwerem**.

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 **Urządzenia** > **Microsoft Exchange**.

   W oprogramowaniu zostanie pokazane drzewo grup dostępności bazy danych (DAG) programu Exchange Server, komputerów z uruchomionym programem Microsoft Exchange Server i baz danych programu Exchange Server. Jeśli agent dla programu Exchange został skonfigurowany zgodnie z opisem podanym w sekcji „Kopia zapasowa skrzynki pocztowej”, w drzewie będą pokazywane również skrzynki pocztowe.
2. Przejdź do danych, które chcesz uwzględnić w kopii zapasowej.

   Rozwiń węzły drzewa lub klikaj dwukrotnie elementy na liście po prawej stronie drzewa.
3. Wybierz dane, które chcesz uwzględnić w kopii zapasowej.
   - W przypadku wybrania grupy DAG w kopii zapasowej znajdzie się jedna kopia każdej klastrowanej bazy danych. Aby uzyskać więcej informacji o tworzeniu kopii zapasowych grup dostępności bazy danych (DAG), zobacz „Ochrona grup dostępności bazy danych (DAG)”.
   - W przypadku wybrania komputera z uruchomionym programem Microsoft Exchange Server w kopii zapasowej zostaną uwzględnione wszystkie bazy danych zamontowane w programie Exchange Server uruchomionym na wybranym komputerze.
   - W przypadku bezpośredniego wybrania baz danych w kopii zapasowej będą uwzględniane tylko wybrane bazy danych.
   - Jeśli agent dla programu Exchange został skonfigurowany zgodnie z opisem podanym w sekcji „Kopia zapasowa skrzynki pocztowej”, można wybrać skrzynki pocztowe do uwzględnienia w kopii zapasowej.
4. Jeśli pojawi się monit, podaj poświadczenia umożliwiające dostęp do danych.
5. Kliknij **Chroń**.

Ochrona zawsze włączonych grup dostępności (AAG)

Przegląd rozwiązań dla serwerów SQL o wysokiej dostępności

Funkcja Windows Server Failover Clustering (WSFC) umożliwia skonfigurowanie serwera SQL o wysokiej dostępności przez zastosowanie nadmiarowości na poziomie instancji (Failover Cluster Instance, FCI) lub na poziomie bazy danych (AlwaysOn Availability Group, AAG). Można również łączyć obie te metody.

W metodzie Failover Cluster Instance bazy danych SQL znajdują się w magazynie współużytkowanym. Do tego magazynu można uzyskać dostęp wyłącznie z aktywnego węzła klastra. W przypadku awarii aktywnego węzła następuje przełączenie awaryjne i aktywny staje się inny węzeł.

W grupie dostępności każda replika bazy danych znajduje się w innym węźle. Jeśli replika główna staje się niedostępna, jej rola jest przypisywana replice dodatkowej znajdującej się w innym węźle.

Dlatego też już same klastry stanowią rozwiązanie odzyskiwania po awarii. Mogą jednak wystąpić sytuacje, kiedy klastry nie mogą zapewnić ochrony danych: na przykład w przypadku logicznego uszkodzenia bazy danych lub uszkodzenia całego klastra. Ponadto rozwiązania klastrowe nie chronią przed szkodliwymi zmianami zawartości, ponieważ zwykle natychmiast replikują dane do wszystkich węzłów klastra.

Obsługiwane konfiguracje klastrów

To oprogramowanie do tworzenia kopii zapasowych obsługuje *wyłącznie* zawsze włączoną grupę dostępności (AAG) w przypadku programu SQL Server 2012 lub nowszego. Inne konfiguracje klastrów, np. instancje klastrów awaryjnych, dublowanie bazy danych i wysyłanie dziennika *nie* są obsługiwane.

Ile agentów jest wymaganych do tworzenia kopii zapasowej i odzyskiwania danych klastra?

Aby pomyślnie utworzyć kopię zapasową danych agenta dla języka SQL i odzyskać ją, w każdym węźle klastra WSFC musi być zainstalowany agent dla języka SQL.

Tworzenie kopii zapasowych baz danych uwzględnionych w grupie AAG

1. Zainstaluj agenta dla języka SQL we wszystkich węzłach klastra WSFC.

   Uwaga
   Po zainstalowaniu agenta w jednym z węzłów oprogramowanie wyświetli grupę AAG i jej węzły w pozycji **Urządzenia** > **Microsoft SQL** > **Bazy danych**. Aby zainstalować agenty dla języka SQL w pozostałych węzłach, wybierz grupę AAG, kliknij pozycję **Szczegóły**, a następnie kliknij opcję **Zainstaluj agenta** obok każdego z węzłów.

2. Wybierz grupę AAG lub zestaw baz danych do uwzględnienia w kopii zapasowej zgodnie z opisem podanym w sekcji „Wybieranie baz danych SQL”.

   Musisz wybrać samą grupę AAG, aby utworzyć kopię zapasową wszystkich jej baz danych. Aby utworzyć kopię zapasową zestawu baz danych, zdefiniuj ten zestaw na wszystkich węzłach grupy AAG.

   Ostrzeżenie!
   Zestaw baz danych musi być dokładnie taki sam na wszystkich węzłach. Jeśli choć jeden zestaw będzie inny lub zestaw nie zostanie zdefiniowany na wszystkich węzłach, operacja tworzenia kopii zapasowej klastra nie przebiegnie poprawnie.

3. Skonfiguruj opcję kopii zapasowej „Tryb tworzenia kopii zapasowych klastra”.

Odzyskiwanie baz danych uwzględnionych w grupie AAG

1. Wybierz bazy danych, które chcesz odzyskać, a następnie wybierz punkt odzyskiwania, z którego chcesz odzyskać bazy danych.

   Jeśli wybierzesz klastrowaną bazę danych w pozycji **Urządzenia** > **Microsoft SQL** > **Bazy danych**, a następnie klikniesz opcję **Odzyskaj**, oprogramowanie wyświetli tylko punkty odzyskiwania związane z czasami, w których utworzono kopię zapasową wybranej kopii bazy danych.

   Najłatwiejszym sposobem na wyświetlenie wszystkich punktów odzyskiwania klastrowanej bazy danych jest wybranie kopii zapasowej całej grupy AAG na karcie Magazyn kopii zapasowych.Kopie zapasowe grupy AAG mają nazwy zgodne z następującym szablonem: `<nazwa grupy AAG> - <nazwa planu ochrony>` i są oznaczane specjalną ikoną.
2. Aby skonfigurować odzyskiwanie, wykonaj kroki opisane w części „Odzyskiwanie baz danych SQL", rozpoczynając od kroku 5.

   Oprogramowanie automatycznie zdefiniuje węzeł klastra, do którego zostaną odzyskane dane. Nazwa węzła jest wyświetlana w polu **Odzyskaj do**. Możesz ręcznie zmienić węzeł docelowy.

   Ważne
   Bazy danych dołączonej do zawsze włączonej grupy dostępności nie można zastąpić podczas odzyskiwania, ponieważ uniemożliwia to program Microsoft SQL Server. Przed rozpoczęciem odzyskiwania należy wykluczyć docelową bazę danych z grupy AAG. Można również odzyskać bazę danych jako nową bazę nie należącą do grupy AAG. Po zakończeniu odzyskiwania można przywrócić oryginalną konfigurację grupy AAG.

Ochrona grup dostępności bazy danych (DAG)

Przegląd klastrów programu Exchange Server

Podstawowym celem stosowania klastrów programu Exchange jest zapewnienie wysokiej dostępności bazy danych, szybkie przełączanie awaryjne i ochrona przed utratą danych. Zwykle osiąga się go przez utworzenie co najmniej jednej kopii baz danych lub grup magazynów w członkach (węzłach) klastra. Jeśli dojdzie do awarii węzła klastra, w którym znajduje się aktywna kopia bazy danych, lub awarii samej aktywnej kopii bazy danych, drugi węzeł, w którym znajduje się pasywna kopia, automatycznie przejmie operacje uszkodzonego węzła i zapewni dostęp do usług programu Exchange z minimalnym czasem przestoju. Dlatego też już same klastry stanowią rozwiązanie odzyskiwania po awarii.

Mogą jednak wystąpić sytuacje, kiedy klastrowe rozwiązania przełączania awaryjnego nie mogą zapewnić ochrony danych, na przykład w przypadku logicznego uszkodzenia bazy danych, braku kopii (repliki) określonej bazy danych w klastrze lub uszkodzenia całego klastra. Ponadto rozwiązania klastrowe nie chronią przed szkodliwymi zmianami zawartości, ponieważ zwykle natychmiast replikują dane do wszystkich węzłów klastra.

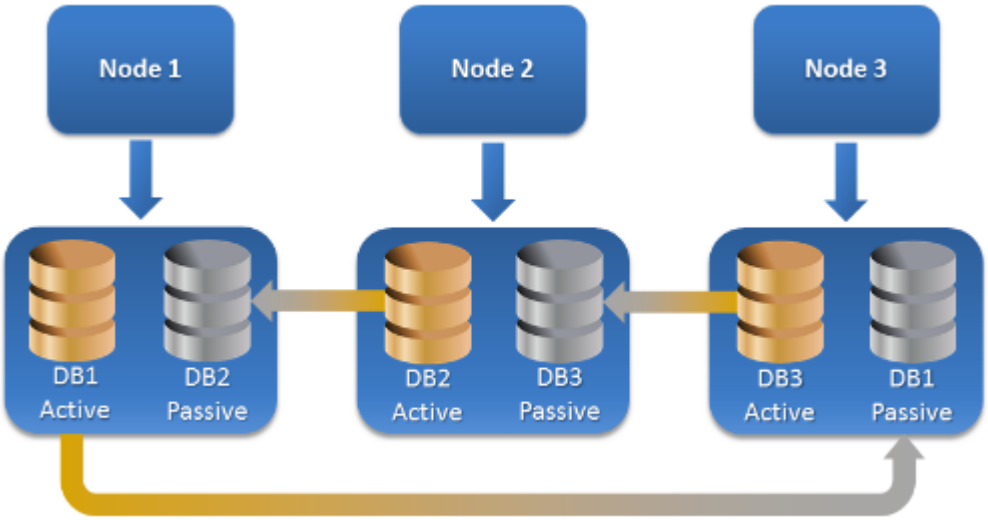
Kopia zapasowa uwzględniająca klastry

W przypadku kopii zapasowej uwzględniającej klastry w kopii zapasowej jest umieszczany tylko jeden egzemplarz danych z klastrów. Jeśli dane zapisywane w kopii zapasowej zmienią swoją lokalizację w klastrze (na przykład w wyniku przełączenia lub przełączenia awaryjnego), program będzie monitorować wszystkie przeniesienia tych danych i bezpiecznie utworzy ich kopię zapasową.

Obsługiwane konfiguracje klastrów

Kopia zapasowa uwzględniająca klastry jest obsługiwana *tylko* w przypadku grupy dostępności bazy danych w programie Exchange Server 2010 lub nowszym. Inne konfiguracje klastrów, np. klastry pojedynczej kopii oraz ciągła replikacja klastra dla programu Exchange 2007, *nie* są obsługiwane.

DAG to grupa maksymalnie 16 serwerów skrzynek pocztowych programu Exchange. Każdy z węzłów może przechowywać kopię bazy danych skrzynki pocztowej z dowolnego z pozostałych węzłów. Każdy z węzłów może przechowywać pasywne i aktywne kopie bazy danych. Możliwe jest utworzenie nawet 16 kopii każdej z baz danych.



Ile agentów potrzeba do utworzenia kopii zapasowej uwzględniającej klastry i odzyskania z niej danych?

Aby pomyślnie utworzyć kopię zapasową klastrowanych baz danych i odzyskać je, w każdym węźle klastra programu Exchange musi być zainstalowany agent dla programu Exchange.

Uwaga
Po zainstalowaniu agenta na jednym z węzłów konsola internetowa Cyber Protect wyświetli grupę DAG i jej węzły w obszarze **Urządzenia** > **Microsoft Exchange** > **Bazy danych**. Aby zainstalować agenty dla programu Exchange w pozostałych węzłach, wybierz grupę DAG, kliknij pozycję **Szczegóły**, a następnie kliknij opcję **Zainstaluj agenta** obok każdego z węzłów.

Tworzenie kopii zapasowej danych klastra programu Exchange

1. Podczas tworzenia planu ochrony wybierz grupę dostępności baz danych zgodnie z opisem podanym w sekcji „Wybieranie danych programu Exchange Server".
2. Skonfiguruj opcję kopii zapasowej „Tryb tworzenia kopii zapasowych klastra".
3. Odpowiednio określ inne ustawienia planu ochrony.

Ważne
W przypadku tworzenia kopii zapasowej uwzględniającej klastry koniecznie wybierz całą grupę dostępności baz danych. Jeśli wybierzesz poszczególne węzły lub bazy danych w tej grupie, w kopii zapasowej zostaną uwzględnione tylko wybrane elementy, a opcja **Tryb tworzenia kopii zapasowych klastra** zostanie zignorowana.

Odzyskiwanie danych klastra programu Exchange

1. Wybierz punkt odzyskiwania dla bazy danych, którą chcesz odzyskać. Nie można wybrać odzyskania całego klastra.

   Jeśli w pozycji **Urządzenia** > **Microsoft Exchange** > **Bazy danych** > `<nazwa klastra>` > `<nazwa węzła>` wybierzesz kopię klastrowanej bazy danych, a następnie klikniesz **Odzyskaj**, oprogramowanie wyświetli tylko punkty odzyskiwania związane z czasami, w których utworzono kopię zapasową wybranej bazy.

   Najłatwiejszym sposobem na wyświetlenie wszystkich punktów odzyskiwania klastrowanej bazy danych jest wybranie jej kopii zapasowej na karcie Magazyn kopii zapasowych.
2. Wykonaj czynności opisane w sekcji „Odzyskiwanie baz danych programu Exchange", rozpoczynając od kroku 5.

   Oprogramowanie automatycznie zdefiniuje węzeł klastra, do którego zostaną odzyskane dane. Nazwa węzła jest wyświetlana w polu **Odzyskaj do**. Możesz ręcznie zmienić węzeł docelowy.

Kopia zapasowa uwzględniająca aplikacje

Uwzględniająca aplikacje kopia zapasowa na poziomie dysku jest dostępna w przypadku komputerów fizycznych, maszyn wirtualnych ESXi i maszyn wirtualnych Hyper-V.

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 ochrony. Dzienniki transakcji programu Exchange są obcinane tylko na maszynach wirtualnych. Jeśli dzienniki transakcji programu Exchange mają być obcinane na komputerze fizycznym, włącz opcję Pełne kopie zapasowe z usługą VSS.
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) lub agenta dla Hyper-V.

Uwaga
W przypadku maszyn wirtualnych Hyper-V z systemem Windows Server 2022 tworzenie kopii zapasowych uwzględniających aplikacje nie jest obsługiwane w trybie bezagentowym, czyli takim, w którym kopia zapasowa jest tworzona przez agenta dla Hyper-V. Aby chronić aplikacje firmy Microsoft na tych maszynach, trzeba zainstalować agenta dla systemu Windows w systemie operacyjnym gościa.

Agent dla VMware (urządzenie wirtualne) i agent dla VMware (Windows) mogą tworzyć kopie zapasowe uwzględniające aplikacje, ale nie mogą odzyskiwać danych aplikacji z tych kopii. Aby odzyskać dane aplikacji z kopii zapasowych utworzonych przez te agenty, potrzebny jest agent dla VMware (Windows), agent dla SQL lub agent dla programu Exchange zainstalowany na komputerze, który ma dostęp do lokalizacji przechowywania tych kopii zapasowych. Konfigurując odzyskiwanie danych aplikacji, wybierz punkt odzyskiwania na karcie **Magazyn kopii zapasowych**, a następnie wybierz dany komputer w polu **Komputer używany do przeglądania**.

Inne wymagania podano w sekcjach "Wymagania wstępne" (s. 457) i "Wymagane prawa użytkownika w przypadku tworzenia kopii zapasowej uwzględniającej aplikacje" (s. 467).

Wymagane prawa użytkownika w przypadku tworzenia kopii zapasowej uwzględniającej aplikacje

Kopia zapasowa uwzględniająca aplikacje zawiera metadane znajdujących się na dysku aplikacji uwzględniających usługę VSS. Aby uzyskać dostęp do tych metadanych, agent potrzebuje konta z odpowiednimi prawami. Wymieniono je poniżej. Podczas włączania tworzenia kopii zapasowej aplikacji pojawi się monit o określenie tego konta.

- W przypadku programu SQL Server:
  W przypadku korzystania z funkcji uwierzytelniania dostępnej w systemie Windows konto musi należeć do grupy **Operatorzy kopii zapasowych** lub **Administratorzy** na danym komputerze oraz do roli **administrator systemu** w każdej instancji uwzględnianej w kopii zapasowej. W przypadku korzystania z funkcji uwierzytelniania dostępnej w programie SQL Server konto musi należeć do roli **administrator systemu** w każdej instancji uwzględnianej w kopii zapasowej.
- W przypadku programu Exchange Server:
  Exchange 2007: Konto musi należeć do grupy **Administratorzy** na komputerze i do grupy z rolą **Administratorzy organizacji korzystającej z programu Exchange**.
  Program Exchange 2010 lub nowszy: Konto musi należeć do grupy **Administratorzy** na komputerze i do grupy z rolą **Zarządzanie organizacją**.
- W przypadku usługi Active Directory:
  Konto musi być administratorem domeny.

Dodatkowe wymaganie dotyczące maszyn wirtualnych

Jeśli aplikacja działa na maszynie wirtualnej, której kopie zapasowe tworzy agent dla VMware lub agent dla Hyper-V, upewnij się, że na tej maszynie jest wyłączona usługa kontroli konta użytkownika. Jeśli nie chcesz wyłączyć usługi UAC, podczas włączania tworzenia kopii zapasowej aplikacji musisz podać poświadczenia wbudowanego administratora domeny (DOMAIN\Administrator).

Dodatkowe wymagania w przypadku komputerów z systemami operacyjnymi Windows

W przypadku każdej wersji systemu Windows trzeba wyłączyć zasady kontroli konta użytkownika, aby można było tworzyć kopie zapasowe uwzględniające aplikacje. Jeśli nie chcesz wyłączyć zasad kontroli użytkownika konta, podczas konfigurowania kopii zapasowych uwzględniających aplikacje koniecznie podaj poświadczenia wbudowanego administratora domeny (DOMAIN\Administrator).

Aby wyłączyć zasady kontroli konta użytkownika w systemie Windows

1. W Edytorze rejestru odszukaj następujący klucz rejestru:
   `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System`

2. Zmień wartość klucza **EnableLUA** na **0**.
3. Uruchom ponownie komputer.

Kopia zapasowa skrzynki pocztowej

Kopia zapasowa skrzynki pocztowej jest obsługiwana w przypadku programu Microsoft Exchange Server 2010 z dodatkiem Service Pack 1 (SP1) lub nowszego.

Kopia zapasowa skrzynki pocztowej jest dostępna, jeśli na serwerze zarządzania jest zarejestrowany przynajmniej jeden agent dla programu Exchange. Agent musi być zainstalowany na komputerze należącym do tego samego lasu usługi Active Directory co program Microsoft Exchange Server.

Przed utworzeniem kopii zapasowej skrzynek pocztowych musisz połączyć agenta dla programu Exchange z komputerem z rolą serwera **Dostęp klienta** (CAS) programu Microsoft Exchange Server. W programie Exchange 2016 lub jego nowszej wersji rola CAS nie jest dostępna jako osobna opcja instalacji. Jest automatycznie instalowana w ramach roli serwera Skrzynka pocztowa. W związku z tym można połączyć agenta z dowolnym serwerem z **rolą Skrzynka pocztowa**.

Aby połączyć agenta dla programu Exchange z CAS

1. Kliknij **Urządzenia** > **Dodaj**.
2. Kliknij opcję **Microsoft Exchange Server**.
3. Kliknij **Skrzynki pocztowe programu Exchange**.
   Jeśli na serwerze zarządzania nie zarejestrowano żadnego agenta dla programu Exchange, oprogramowanie zasugeruje zainstalowanie tego agenta. Po zakończeniu instalacji powtórz procedurę, zaczynając od kroku 1.
4. [Opcjonalnie] Jeśli na serwerze zarządzania zarejestrowano kilka agentów dla programu Exchange, kliknij **Agent**, a następnie zmień agenta, które utworzy kopię zapasową.
5. W sekcji **Serwer dostępu klienta** określ w pełni kwalifikowaną nazwę domeny (FQDN) komputera z rolą **Dostęp klienta** programu Microsoft Exchange Server.
   W programie Exchange 2016 lub jego nowszej wersji usługi dostępu klienta są automatycznie instalowane w ramach roli serwera Skrzynka pocztowa. W związku z tym można określić dowolny serwer z **rolą Skrzynka pocztowa**. W dalszej części tej sekcji ten serwer jest określany jako serwer CAS.
6. W sekcji **Typ uwierzytelniania** wybierz typ uwierzytelniania, który jest używany przez serwer CAS. Możesz wybrać typ **Kerberos** (domyślny) lub **Podstawowe**.
7. [Tylko w przypadku uwierzytelniania podstawowego] Wybierz protokół, który będzie używany. Możesz wybrać protokół **HTTP** (domyślny) lub **HTTPS**.
8. [Tylko w przypadku uwierzytelniania podstawowego przy użyciu protokołu HTTPS] Jeśli serwer CAS korzysta z certyfikatu SSL uzyskanego od podmiotu certyfikującego i chcesz, aby oprogramowanie sprawdzało ten certyfikat podczas nawiązywania połączenia z serwerem CAS, zaznacz pole wyboru **Sprawdź certyfikat SSL**. W przeciwnym razie pomiń ten krok.
9. Określ poświadczenia konta, które będzie używane w celu uzyskania dostępu do serwera CAS.

Wymagania wobec takiego konta znajdują się w sekcji „Wymagane prawa użytkownika”.

10. Kliknij **Dodaj**.

Wskutek tego skrzynki pocztowe pojawią się w pozycji **Urządzenia** > **Microsoft Exchange** > **Skrzynki pocztowe**.

Wybieranie skrzynek pocztowych programu Exchange Server

Wybierz skrzynki pocztowe zgodnie z poniższym opisem, a następnie odpowiednio określ inne ustawienia planu ochrony.

Aby wybrać skrzynki pocztowe programu Exchange

1. Kliknij **Urządzenia** > **Microsoft Exchange**.
   Program wyświetli drzewo baz danych programu Exchange i skrzynek pocztowych.
2. Kliknij **Skrzynki pocztowe**, a następnie wybierz skrzynki pocztowe, które chcesz uwzględnić w kopii zapasowej.
3. Kliknij **Kopia zapasowa**.

Wymagane prawa użytkownika

Aby uzyskać dostęp do skrzynek pocztowych, agent do programu Exchange potrzebuje konta z odpowiednimi uprawnieniami. Podczas konfigurowania różnych operacji na skrzynkach pocztowych pojawi się monit o określenie tego konta.

Przynależność konta do grupy z rolą **zarządzania organizacją** pozwala uzyskać dostęp do każdej skrzynki pocztowej, również do skrzynek tworzonych w przyszłości.

Minimalne wymagane prawa użytkownika:

- Konto musi należeć do grup ról **Zarządzanie serwerem** i **Zarządzanie odbiorcami**.
- Konto musi mieć rolę **ApplicationImpersonation** i musi być ona włączona dla wszystkich użytkowników lub grup użytkowników, do których skrzynek pocztowych agent będzie mieć dostęp.
  Aby uzyskać informacje na temat konfiguracji roli zarządzania **ApplicationImpersonation**, przeczytaj następujący artykuł bazy wiedzy firmy Microsoft: https://msdn.microsoft.com/en-us/library/office/dn722376.aspx.

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.

W przypadku korzystania z funkcji uwierzytelniania dostępnej w systemie Windows trzeba będzie podać poświadczenia konta należącego do grupy **Operatorzy kopii zapasowych** lub **Administratorzy** na danym komputerze oraz do roli **administratora systemu** w instancji docelowej. W przypadku korzystania z funkcji uwierzytelniania dostępnej w programie SQL Server trzeba będzie podać poświadczenia konta należącego do roli **administratora systemu** w instancji docelowej.

Można też odzyskać bazy danych jako pliki. Może się to przydać w przypadku, gdy trzeba wyodrębnić dane w celu ich przeanalizowania, 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”.

Jeśli używasz tylko agenta dla VMware (system Windows), jedyną dostępną metodą odzyskiwania jest odzyskiwanie baz danych jako plików. Nie można odzyskiwać baz danych za pomocą agenta dla VMware (urządzenie wirtualne).

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”.

Aby odzyskać bazy danych SQL do instancji serwera SQL

1. Wykonaj jedną z następujących czynności:
   - W przypadku odzyskiwania z kopii zapasowej uwzględniającej aplikacje w obszarze **Urządzenia** wybierz komputer pierwotnie zawierający dane, które chcesz odzyskać.
   - W przypadku odzyskiwania z kopii zapasowej bazy danych kliknij **Urządzenia** > **Microsoft SQL**, a następnie wybierz bazy danych, które chcesz odzyskać.
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 jedną z następujących czynności:
   - [Tylko w przypadku odzyskiwania z kopii zapasowej uwzględniającej aplikacje] Jeśli lokalizacja kopii zapasowej to chmura lub współużytkowany magazyn (czyli inni agenci mogą uzyskiwać do niej dostęp), kliknij **Wybierz komputer**, wybierz komputer z agentem dla SQL będący w trybie online, a następnie wybierz punkt odzyskiwania.
   - Wybierz punkt odzyskiwania na karcie Magazyn kopii zapasowych.

   Komputer wybrany do przeglądania w ramach jednej z powyższych czynności staje się komputerem docelowym odzyskiwania baz danych SQL.
4. Wykonaj jedną z następujących czynności:
   - W przypadku odzyskiwania z kopii zapasowej uwzględniającej aplikacje kliknij **Odzyskaj** > **Bazy danych SQL**, wybierz bazy danych, które chcesz odzyskać, a następnie kliknij **Odzyskaj**.
   - W przypadku odzyskiwania z kopii zapasowej bazy danych kliknij **Odzyskaj** > **Bazy danych do instancji**.

5. Domyślnie program odzyska bazy danych do pierwotnej lokalizacji. Jeśli pierwotna baza danych nie istnieje, zostanie odtworzona. Program umożliwia wybór innej instancji serwera SQL (działającej na tym samym komputerze), do której 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.
6. [Opcjonalnie] [Działanie niedostępne w przypadku bazy danych odzyskanej do jej pierwotnej instancji jako nowa baza danych] 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.
7. Kliknij **Rozpocznij odzyskiwanie**.

Na karcie **Działania** jest wyświetlany postęp odzyskiwania.

Aby odzyskać bazy danych SQL jako pliki

1. Wykonaj jedną z następujących czynności:
   - W przypadku odzyskiwania z kopii zapasowej uwzględniającej aplikacje w obszarze **Urządzenia** wybierz komputer pierwotnie zawierający dane, które chcesz odzyskać.
   - W przypadku odzyskiwania z kopii zapasowej bazy danych kliknij **Urządzenia** > **Microsoft SQL**, a następnie wybierz bazy danych, które chcesz odzyskać.
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 jedną z następujących czynności:

- [Tylko w przypadku odzyskiwania z kopii zapasowej uwzględniającej aplikacje] Jeśli lokalizacja kopii zapasowej to chmura lub współużytkowany magazyn (czyli inni agenci mogą uzyskiwać do niej dostęp), kliknij **Wybierz komputer**, wybierz komputer z agentem dla SQL lub agentem dla VMware będący w trybie online, a następnie wybierz punkt odzyskiwania.
- Wybierz punkt odzyskiwania na karcie Magazyn kopii zapasowych.

Komputer wybrany do przeglądania w ramach jednej z powyższych czynności staje się komputerem docelowym odzyskiwania baz danych SQL.

4. Wykonaj jedną z następujących czynności:
   - W przypadku odzyskiwania z kopii zapasowej uwzględniającej aplikacje kliknij **Odzyskaj** > **Bazy danych SQL**, wybierz bazy danych, które chcesz odzyskać, a następnie kliknij **Odzyskaj jako pliki**.
   - W przypadku odzyskiwania z kopii zapasowej bazy danych kliknij **Odzyskaj** > **Bazy danych jako pliki**.
5. Kliknij **Przeglądaj**, a następnie wybierz folder lokalny lub sieciowy, w którym mają zostać zapisane pliki.
6. Kliknij **Rozpocznij odzyskiwanie**.

Na karcie **Działania** jest wyświetlany postęp odzyskiwania.

Odzyskiwanie systemowych baz danych

Program odzyska wszystkie systemowe bazy danych instancji jednocześnie. Podczas odzyskiwania systemowych baz danych oprogramowanie automatycznie uruchamia ponownie instancję docelową 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.

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. Kliknij prawym przyciskiem myszy **Bazy danych** i kliknij **Dołącz**.
4. Kliknij **Dodaj**.
5. W oknie dialogowym **Odszukaj pliki bazy danych** znajdź i wybierz plik .mdf bazy danych.
6. W sekcji **Szczegóły bazy danych** sprawdź, czy zostały znalezione pozostałe pliki bazy danych (pliki .ndf i .ldf).

   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 zostaną znalezione wszystkie pliki, kliknij **OK**.

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	Elementy	Prawa użytkownika

Exchange	danych	
2007	Grupy magazynów	Członkostwo w grupie z rolą **Administratorzy organizacji korzystającej z programu Exchange**.
2010/2013/2016/2019	Bazy danych	Członkostwo w grupie z rolą **Zarządzanie serwerem**.

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.

Jeśli używasz tylko agenta dla VMware (system Windows), jedyną dostępną metodą odzyskiwania jest odzyskiwanie baz danych jako plików. Nie można odzyskiwać baz danych za pomocą agenta dla VMware (urządzenie wirtualne).

W przypadku poniższych procedur pojęcie „bazy danych" dotyczy zarówno baz danych, jak i grup magazynów.

Aby odzyskać bazy danych programu Exchange do działającego programu Exchange Server

1. Wykonaj jedną z następujących czynności:
   - W przypadku odzyskiwania z kopii zapasowej uwzględniającej aplikacje w obszarze **Urządzenia** wybierz komputer pierwotnie zawierający dane, które chcesz odzyskać.
   - W przypadku odzyskiwania z kopii zapasowej bazy danych kliknij **Urządzenia** > **Microsoft Exchange** > **Bazy danych**, a następnie wybierz bazy danych, które chcesz odzyskać.
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 jedną z następujących czynności:
   - [Tylko w przypadku odzyskiwania z kopii zapasowej uwzględniającej aplikacje] Jeśli lokalizacja kopii zapasowej to chmura lub współużytkowany magazyn (czyli inni agenci mogą uzyskiwać do niej dostęp), kliknij **Wybierz komputer**, wybierz komputer z agentem dla programu Exchange będący w trybie online, a następnie wybierz punkt odzyskiwania.
   - Wybierz punkt odzyskiwania na karcie Magazyn kopii zapasowych.

   Komputer wybrany do przeglądania w ramach jednej z powyższych czynności staje się komputerem docelowym odzyskiwania danych programu Exchange.
4. Wykonaj jedną z następujących czynności:
   - W przypadku odzyskiwania z kopii zapasowej uwzględniającej aplikacje kliknij **Odzyskaj** > **Bazy danych programu Exchange**, wybierz bazy danych, które chcesz odzyskać, a następnie kliknij **Odzyskaj**.
   - W przypadku odzyskiwania z kopii zapasowej bazy danych kliknij opcję **Odzyskaj** > **Bazy danych do serwera programu Exchange**.

5. 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.

6. Kliknij **Rozpocznij odzyskiwanie**.

Na karcie **Działania** jest wyświetlany postęp odzyskiwania.

Aby odzyskać bazy danych programu Exchange jako pliki

1. Wykonaj jedną z następujących czynności:
   - W przypadku odzyskiwania z kopii zapasowej uwzględniającej aplikacje w obszarze **Urządzenia** wybierz komputer pierwotnie zawierający dane, które chcesz odzyskać.
   - W przypadku odzyskiwania z kopii zapasowej bazy danych kliknij **Urządzenia** > **Microsoft Exchange** > **Bazy danych**, a następnie wybierz bazy danych, które chcesz odzyskać.
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 jedną z następujących czynności:
   - [Tylko w przypadku odzyskiwania z kopii zapasowej uwzględniającej aplikacje] Jeśli lokalizacją kopii zapasowej jest chmura lub współużytkowany magazyn (czyli inne agenty mogą uzyskiwać do niej dostęp), kliknij **Wybierz komputer**, wybierz komputer z agentem dla programu Exchange lub agentem dla VMware będący w trybie online, a następnie wybierz punkt odzyskiwania.
   - Wybierz punkt odzyskiwania na karcie Magazyn kopii zapasowych.

   Komputer wybrany do przeglądania w ramach jednej z powyższych czynności staje się komputerem docelowym odzyskiwania danych programu Exchange.
4. Wykonaj jedną z następujących czynności:
   - W przypadku odzyskiwania z kopii zapasowej uwzględniającej aplikacje kliknij **Odzyskaj** > **Bazy danych programu Exchange**, wybierz bazy danych, które chcesz odzyskać, a następnie kliknij **Odzyskaj jako pliki**.
   - W przypadku odzyskiwania z kopii zapasowej bazy danych kliknij **Odzyskaj** > **Bazy danych jako pliki**.
5. Kliknij **Przeglądaj**, a następnie wybierz folder lokalny lub sieciowy, w którym mają zostać zapisane pliki.
6. Kliknij **Rozpocznij odzyskiwanie**.

Na karcie **Działania** jest wyświetlany postęp odzyskiwania.

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 (takiej jak nowa baza danych lub baza danych odzyskiwania) jej zamontowanie jest możliwe dopiero po przywróceniu 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 którego 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 w wersji 2010 lub nowszej: http://technet.microsoft.com/en-us/library/aa998871.aspx
- Program Exchange w wersji 2007: http://technet.microsoft.com/en-us/library/aa998871(v=EXCHG.80).aspx

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, a także z kopii zapasowych skrzynek pocztowych. Skrzynki pocztowe lub elementy skrzynek pocztowych można odzyskać na aktywny serwer Exchange Server lub do usługi Microsoft 365.

Można odzyskać następujące elementy:

- Skrzynki pocztowe (z wyjątkiem archiwalnych skrzynek pocztowych)
- Foldery publiczne

  Uwaga
  Dostępne tylko z kopii zapasowych baz danych. Zobacz "Wybieranie danych programu Exchange Server" (s. 460)

- Elementy folderu publicznego
- Foldery poczty e-mail
- Wiadomości e-mail

- Zdarzenia kalendarza
- Zadania
- Kontakty
- Wpisy dziennika
- Notatki

Elementy można znaleźć przy użyciu funkcji wyszukiwania.

Odzyskiwanie na serwer Exchange Server

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 lub skrzynki pocztowe 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.

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. Zamiast tego w folderze docelowym zostanie odtworzona pełna ścieżka elementu 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.

Odzyskiwanie do usługi Microsoft 365

Odzyskiwanie jest możliwe tylko w przypadku kopii zapasowych programu Microsoft Exchange Server 2010 lub nowszego.

W przypadku odzyskiwania skrzynki pocztowej do istniejącej już skrzynki Microsoft 365 dostępne w niej elementy pozostają niezmienione, a odzyskane elementy zostają po prostu dodane.

W przypadku odzyskiwania jednej skrzynki pocztowej należy wybrać docelową skrzynkę pocztową Microsoft 365. W przypadku odzyskiwania kilku skrzynek pocztowych w ramach jednej operacji program spróbuje odzyskać każdą skrzynkę do skrzynki użytkownika o tej samej nazwie. W razie nieznalezienia danego użytkownika skrzynka pocztowa zostanie pominięta. W przypadku pominięcia niektórych skrzynek pocztowych odzyskiwanie zakończy się powodzeniem z ostrzeżeniami. W przypadku pominięcia wszystkich skrzynek pocztowych odzyskiwania zakończy się niepowodzeniem.

Dodatkowe informacje na temat odzyskiwania do usługi Microsoft 365 można znaleźć w sekcji "Ochrona skrzynek pocztowych Microsoft 365" (s. 485).

Odzyskiwanie skrzynek pocztowych

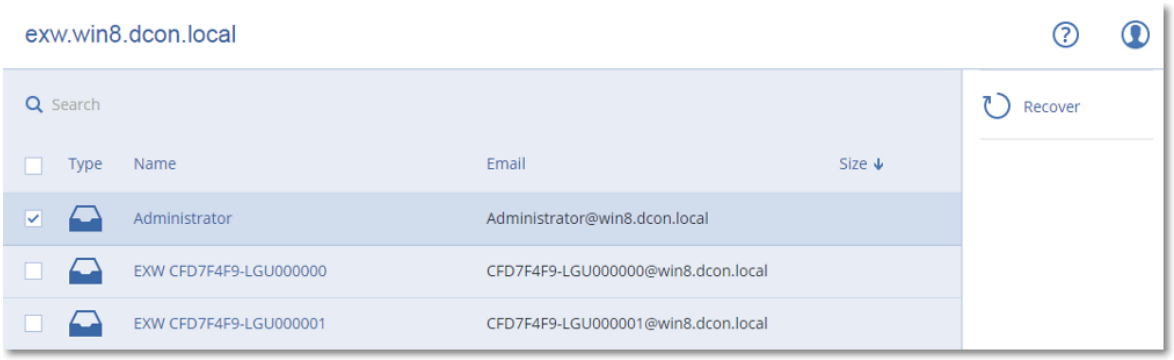
Aby odzyskać skrzynki pocztowe z kopii zapasowej uwzględniającej aplikacje lub kopii zapasowej bazy danych

1. [Tylko w przypadku odzyskiwania z kopii zapasowej bazy danych do usługi Microsoft 365] Jeśli na komputerze z programem Exchange Server uwzględnionym w kopii zapasowej nie jest zainstalowany agent dla usługi Office 365, wykonaj jedną z następujących czynności:
   - Jeśli w Twojej organizacji nie ma agenta dla usługi Office 365, zainstaluj go na komputerze uwzględnionym w kopii zapasowej (lub innym komputerze z tą samą wersją programu Microsoft Exchange Server).
   - Jeśli w organizacji już jest agent dla usługi Office 365, skopiuj biblioteki z komputera uwzględnionego w kopii zapasowej (lub innego komputera z tą samą wersją programu Microsoft Exchange Server) na komputer z tym agentem, postępując zgodnie z opisem podanym w sekcji „Kopiowanie bibliotek programu Microsoft Exchange”.
2. Wykonaj jedną z następujących czynności:
   - W przypadku odzyskiwania z kopii zapasowej uwzględniającej aplikacje w obszarze **Urządzenia** wybierz komputer pierwotnie zawierający dane, które chcesz odzyskać.
   - W przypadku odzyskiwania z kopii zapasowej bazy danych kliknij **Urządzenia** > **Microsoft Exchange** > **Bazy danych**, a następnie wybierz bazę danych pierwotnie zawierającą dane, które chcesz odzyskać.
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:
   - [Tylko w przypadku odzyskiwania z kopii zapasowej uwzględniającej aplikacje] Jeśli lokalizacją kopii zapasowej jest chmura lub współużytkowany magazyn (czyli inne agenty mogą uzyskiwać do niej dostęp), kliknij **Wybierz komputer**, wybierz komputer z agentem dla programu Exchange lub agentem dla VMware będący w trybie online, a następnie wybierz punkt odzyskiwania.
   - Wybierz punkt odzyskiwania na karcie Magazyn kopii zapasowych.

   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. [Tylko w przypadku odzyskiwania do usługi Microsoft 365]:
   a. W polu **Odzyskaj do** wybierz **Microsoft Office 365**.
   b. [Jeśli w kroku 6 została wybrana tylko jedna skrzynka pocztowa] W polu **Docelowa skrzynka pocztowa** określ docelową skrzynkę pocztową.
   c. Kliknij **Rozpocznij odzyskiwanie**.

   Kolejne kroki tej procedury nie są wymagane.
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.

   Podaj w pełni kwalifikowaną nazwę domeny (FQDN) komputera, na którym jest włączona rola **Dostęp klienta** (w przypadku programu Microsoft Exchange Server 2010/2013) lub **rola Skrzynka pocztowa** (w przypadku programu Microsoft Exchange Server 2016 lub nowszego). Komputer musi należeć do tego samego lasu usługi Active Directory co komputer wykonujący operację odzyskiwania.

   Jeśli pojawi się stosowny monit, określ poświadczenia konta, które będzie używane w celu uzyskania dostępu do komputera. Wymagania dotyczące takiego konta można znaleźć w sekcji "Wymagane prawa użytkownika" (s. 469).
10. [Opcjonalnie] Kliknij **Baza danych używana do odtworzenia brakujących skrzynek pocztowych**, aby zmienić automatycznie wybraną bazę danych.
11. Kliknij **Rozpocznij odzyskiwanie**.

Na karcie **Działania** jest wyświetlany postęp odzyskiwania.

Aby odzyskać skrzynkę pocztową z kopii zapasowej skrzynek pocztowych

1. Kliknij kolejno **Urządzenia** > **Microsoft Exchange** > **Skrzynki pocztowe**.
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, zaznacz ją na karcie Magazyn kopii zapasowych, a następnie kliknij **Pokaż kopie zapasowe**.

3. Wybierz punkt odzyskiwania. Uwaga, punkty odzyskiwania są filtrowane na podstawie lokalizacji.
4. Kliknij **Odzyskaj** > **Skrzynka pocztowa**.
5. Wykonaj kroki 8–11 powyższej procedury.

Odzyskiwanie elementów skrzynki pocztowej

Aby odzyskać elementy skrzynki pocztowej z kopii zapasowej uwzględniającej aplikacje lub kopii zapasowej bazy danych

1. [Tylko w przypadku odzyskiwania z kopii zapasowej bazy danych do usługi Microsoft 365] Jeśli na komputerze z programem Exchange Server uwzględnionym w kopii zapasowej nie jest zainstalowany agent dla usługi Office 365, wykonaj jedną z następujących czynności:
   - Jeśli w Twojej organizacji nie ma agenta dla usługi Office 365, zainstaluj go na komputerze uwzględnionym w kopii zapasowej (lub innym komputerze z tą samą wersją programu Microsoft Exchange Server).
   - Jeśli w organizacji już jest agent dla usługi Office 365, skopiuj biblioteki z komputera uwzględnionego w kopii zapasowej (lub innego komputera z tą samą wersją programu Microsoft Exchange Server) na komputer z tym agentem, postępując zgodnie z opisem podanym w sekcji „Kopiowanie bibliotek programu Microsoft Exchange”.
2. Wykonaj jedną z następujących czynności:
   - W przypadku odzyskiwania z kopii zapasowej uwzględniającej aplikacje w obszarze **Urządzenia** wybierz komputer pierwotnie zawierający dane, które chcesz odzyskać.
   - W przypadku odzyskiwania z kopii zapasowej bazy danych kliknij **Urządzenia** > **Microsoft Exchange** > **Bazy danych**, a następnie wybierz bazę danych pierwotnie zawierającą dane, które chcesz odzyskać.
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:
   - [Tylko w przypadku odzyskiwania z kopii zapasowej uwzględniającej aplikacje] Jeśli lokalizacją kopii zapasowej jest chmura lub współużytkowany magazyn (czyli inne agenty mogą uzyskiwać do niej dostęp), kliknij **Wybierz komputer**, wybierz komputer z agentem dla programu Exchange lub agentem dla VMware będący w trybie online, a następnie wybierz punkt odzyskiwania.
   - Wybierz punkt odzyskiwania na karcie Magazyn kopii zapasowych.

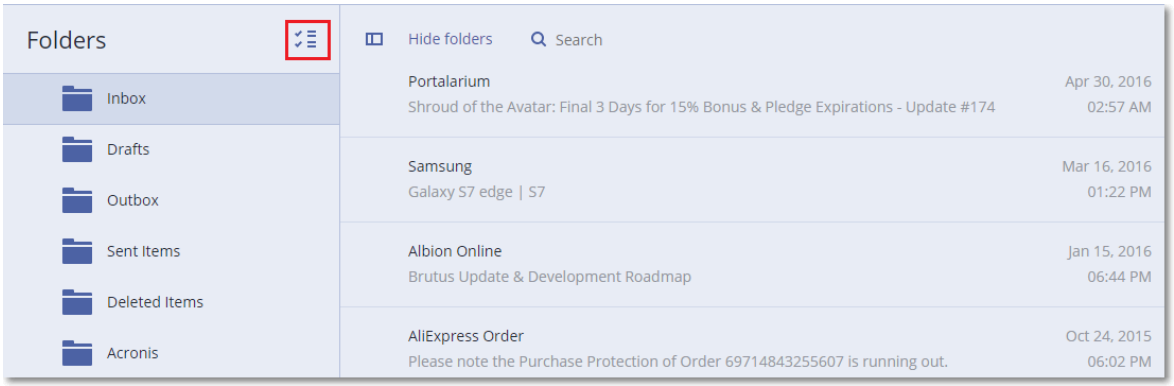
   Komputer wybrany do przejrzenia w ramach dowolnego z powyższych działań wykona operację odzyskiwania w zastępstwie pierwotnego komputera będącego w trybie offline.
5. Kliknij **Odzyskaj** > **Skrzynki pocztowe programu Exchange**.
6. Kliknij skrzynkę pocztową, która pierwotnie zawierała elementy do odzyskania.
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.

Uwaga
Kliknij nazwę załączonego pliku, aby go pobrać.

Aby mieć możliwość wybrania folderów, kliknij ikonę odzyskiwania folderów.



8. Kliknij **Odzyskaj**.
9. Aby odzyskać dane do usługi Microsoft 365, wybierz **Microsoft Office 365** w polu **Odzyskaj do**.
   Aby odzyskać na serwer Exchange Server, zachowaj wartość domyślną **Microsoft Exchange** w polu **Odzyskaj do**.
10. [Tylko w przypadku odzyskiwania na serwer Exchange Server] 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.
    Podaj w pełni kwalifikowaną nazwę domeny (FQDN) komputera, na którym jest włączona rola **Dostęp klienta** (w przypadku programu Microsoft Exchange Server 2010/2013) lub **rola Skrzynka pocztowa** (w przypadku programu Microsoft Exchange Server 2016 lub nowszego). Komputer musi należeć do tego samego lasu usługi Active Directory co komputer wykonujący operację odzyskiwania.
    Jeśli pojawi się stosowny monit, określ poświadczenia konta, które będzie używane w celu uzyskania dostępu do komputera. Wymagania dotyczące takiego konta można znaleźć w sekcji "Wymagane prawa użytkownika" (s. 469).
11. 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.
12. [Tylko w przypadku odzyskiwania wiadomości e-mail] W polu **Folder docelowy** wyświetl lub zmień folder docelowy w docelowej skrzynce pocztowej. Domyślnie wybrany jest folder **Odzyskane elementy**. Ze względu na ograniczenia programu Microsoft Exchange zdarzenia,

zadania, notatki i kontakty są przywracane do pierwotnej lokalizacji, nawet jeśli w polu **Folder docelowy** podano inną lokalizację.

13. Kliknij **Rozpocznij odzyskiwanie**.

Na karcie **Działania** jest wyświetlany postęp odzyskiwania.

Aby odzyskać skrzynkę pocztową z kopii zapasowej skrzynek pocztowych

1. Kliknij kolejno **Urządzenia** > **Microsoft Exchange** > **Skrzynki pocztowe**.
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, zaznacz ją na karcie Magazyn kopii zapasowych, 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.
   - 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.

   Uwaga
   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 odzyskiwania folderów: 
6. Kliknij **Odzyskaj**.
7. Wykonaj kroki 9–13 powyższej procedury.

Kopiowanie bibliotek programu Microsoft Exchange Server

W przypadku odzyskiwania skrzynek pocztowych programu Exchange lub ich elementów do usługi Microsoft 365 może być konieczne skopiowanie poniższych bibliotek z komputera uwzględnionego w kopii zapasowej (lub innego komputera z tą samą wersją programu Microsoft Exchange Server) na komputer z agentem dla usługi Office 365.

Skopiuj poniższe pliki, zgodnie z wersją programu Microsoft Exchange Server uwzględnioną w kopii zapasowej.

Wersja serwera Microsoft Exchange Server	Biblioteki	Lokalizacja domyślna
Microsoft Exchange Server 2010	ese.dll esebcli2.dll store.exe	%ProgramFiles%\Microsoft\Exchange Server\V14\bin
Microsoft Exchange Server 2013	ese.dll	%ProgramFiles%\Microsoft\Exchange Server\V15\bin
	msvcr110.dll	%WINDIR%\system32
Microsoft Exchange Server 2016, 2019	ese.dll	%ProgramFiles%\Microsoft\Exchange Server\V15\bin
	msvcr110.dll msvcp110.dll	%WINDIR%\system32

Biblioteki powinny zostać umieszczone w folderze **%ProgramData%\Acronis\ese**. Jeśli taki folder nie istnieje, utwórz go ręcznie.

Zmiana poświadczeń dostępu programu SQL Server lub Exchange Serwer

Możesz zmienić poświadczenia dostępu dla programu SQL Server lub Exchange Server bez ponownej instalacji agenta.

Aby zmienić poświadczenia dostępu programu SQL Server lub Exchange Serwer

1. Kliknij **Urządzenia**, a następnie kliknij **Microsoft SQL** lub **Microsoft Exchange**.
2. Wybierz zawsze włączoną grupę dostępności, grupę dostępności bazy danych, instancję serwera SQL lub serwer Exchange, w których przypadku chcesz zmienić poświadczenia dostępu.
3. Kliknij **Określ poświadczenia**.
4. Określ nowe poświadczenia dostępu, a następnie kliknij **OK**.

Aby zmienić poświadczenia dostępu serwera Exchange Serwer dla kopii zapasowej skrzynki pocztowej

1. Kliknij **Urządzenia** > **Microsoft Exchange** i rozwiń węzeł **Skrzynki pocztowe**.
2. Wybierz program Exchange Server, dla którego chcesz zmienić poświadczenia dostępu.
3. Kliknij **Ustawienia**.

4. W obszarze **Konto administratora programu Exchange** określ nowe poświadczenia dostępu, a następnie kliknij **Zapisz**.

Ochrona skrzynek pocztowych Microsoft 365

Ważne
Ta sekcja dotyczy lokalnych wdrożeń programu Acronis Cyber Protect. W przypadku wdrożenia chmurowego skorzystaj z artykułu https://www.acronis.com/support/documentation/CyberProtectionService/#protecting-microsoft-365-data.html.

Aby uzyskać dodatkowe informacje na temat opcji licencjonowania, zobacz Licencjonowanie programu Acronis Cyber Backup dla pakietu Microsoft 365.

Dlaczego warto tworzyć kopie zapasowe skrzynek pocztowych Microsoft 365?

Wprawdzie Microsoft 365 jest usługą chmurową, jednak 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 upłynięciu okresu ich przechowywania w usłudze Microsoft 365. Można też przechowywać lokalną kopię skrzynek pocztowych Microsoft 365, jeśli wymagają tego obowiązujące przepisy prawa.

Odzyskiwanie

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.

Dane można odzyskać do usługi Microsoft 365 lub na aktywny serwer programu Exchange.

W przypadku odzyskiwania skrzynki pocztowej do już istniejącej skrzynki Microsoft 365 dostępne w niej elementy o takich samych identyfikatorach zostaną zastąpione. W przypadku odzyskiwania skrzynki pocztowej do używanej skrzynki na serwerze Exchange Server dostępne w niej elementy pozostaną nienaruszone. Odzyskane elementy zostaną po prostu dodane.

Odzyskiwanie elementów skrzynki pocztowej nie powoduje zastępowania żadnych danych. Zamiast tego w folderze docelowym zostanie odtworzona pełna ścieżka elementu skrzynki pocztowej.

Ograniczenia

- Zastosowanie planu ochrony do ponad 500 skrzynek pocztowych może skutkować spadkiem wydajności tworzenia kopii zapasowych. Aby zadbać o ochronę dużej liczby skrzynek pocztowych, warto utworzyć kilka planów ochrony i zaplanować ich uruchomienie w różnym czasie.
- Nie można tworzyć kopii zapasowych archiwalnych skrzynek pocztowych (**archiwum zbiorczego**).
- Kopia zapasowa skrzynek pocztowych obejmuje tylko foldery widoczne dla użytkowników. Folder **Elementy odzyskiwalne** i jego podfoldery (**Usunięcia**, **Wersje**, **Oczyszczone**, **Audyty**, **DiscoveryHold**, **Rejestrowanie kalendarza**] nie są uwzględniane w kopii zapasowej.
- Odzyskanie danych do nowej skrzynki pocztowej Microsoft 365 nie jest możliwe. Trzeba najpierw ręcznie utworzyć nowego użytkownika usługi Microsoft 365, a następnie odzyskać elementy do jego skrzynki pocztowej.
- Odzyskiwanie danych do innej organizacji Microsoft 365 nie jest obsługiwane.
- Niektóre typy elementów lub właściwości obsługiwane przez usługę Microsoft 365 mogą nie być obsługiwane przez serwer programu Exchange. Podczas odzyskiwania na serwer Exchange Server zostaną one pominięte.

Dodawanie organizacji Microsoft 365

Aby dodać organizację Microsoft, trzeba znać identyfikator i klucz tajny aplikacji oraz identyfikator dzierżawcy Microsoft 365. Więcej informacji na temat ich lokalizacji można znaleźć w sekcji Uzyskiwanie identyfikatora i klucza tajnego aplikacji.

Aby dodać organizację Microsoft 365

1. 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.
2. W konsoli internetowej Cyber Protect kliknij **Microsoft Office 365**.
3. W otwartym oknie wprowadź identyfikator i klucz tajny aplikacji oraz identyfikator dzierżawcy Microsoft 365.
4. Kliknij **Zaloguj się**.

W wyniku tych działań elementy danych organizacji pojawią się w konsoli internetowej Cyber Protect na karcie **Microsoft Office 365**.

Uzyskiwanie identyfikatora i klucza tajnego aplikacji

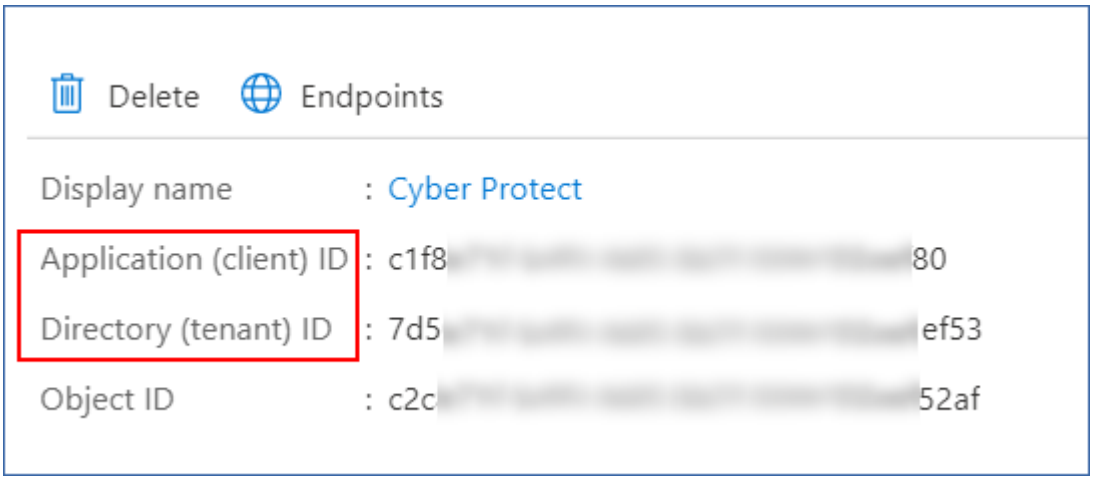
Aby korzystać z nowoczesnej technologii uwierzytelniania w usłudze Microsoft 365, trzeba utworzyć aplikację niestandardową w Azure Active Directory i nadać jej określone uprawnienia do interfejsów

API. W ten sposób uzyskasz **identyfikator aplikacji**, **klucz tajny aplikacji** oraz **identyfikator katalogu (dzierżawcy)**, które trzeba wprowadzić w konsoli internetowej Cyber Protect.

Aby utworzyć aplikację w Azure Active Directory

1. Zaloguj się w portalu Azure jako administrator.
2. Przejdź do sekcji **Azure Active Directory** > **Rejestracje aplikacji** i kliknij **Nowa rejestracja**.
3. Określ nazwę aplikacji niestandardowej, na przykład Cyber Protect.
4. W polu **Obsługiwane typy kont** zaznacz **Tylko konta w tym katalogu organizacyjnym**.
5. Kliknij **Zarejestruj**.

Aplikacja została utworzona. W portalu Azure przejdź do strony **Przegląd** aplikacji i sprawdź jej identyfikator (klienta) oraz katalog (identyfikator dzierżawcy).



Więcej informacji na temat tworzenia aplikacji w portalu Azure można znaleźć w dokumentacji firmy Microsoft.

Aby przyznaj aplikacji niezbędne uprawnienia do interfejsów API

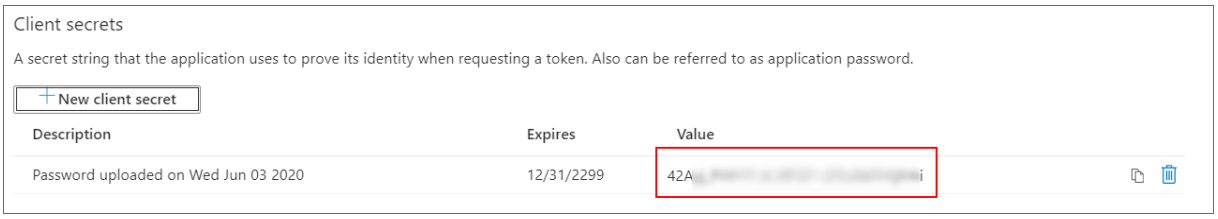
1. W portalu Azure przejdź do sekcji **Uprawnienia interfejsu API** aplikacji i kliknij **Dodaj uprawnienie**.
2. Wybierz kartę **Interfejsy API, z których korzysta moja organizacja** i wyszukaj **Office 365 Exchange Online**.
3. Kliknij **Office 365 Exchange Online**, a następnie kliknij **Uprawnienia aplikacji**.
4. Zaznacz pole wyboru **full_access_as_app** i kliknij **Dodaj uprawnienia**.
5. W polu **Uprawnienia interfejsu API** kliknij **Dodaj uprawnienie**.
6. Wybierz **Microsoft Graph**.
7. Wybierz **Uprawnienia aplikacji**.
8. Rozwiń kartę **Katalog** i zaznacz pole wyboru **Directory.Read.All**. Kliknij **Dodaj uprawnienia**.
9. Sprawdź wszystkie uprawnienia i kliknij **Przyznaj zgodę administratora na rejestrację**

aplikacji <nazwa aplikacji>.

10. Potwierdź wybór, klikając **Tak**.

Aby utworzyć klucz tajny aplikacji

1. W portalu Azure przejdź do sekcji **Certyfikaty i klucze tajne** > **Nowy klucz tajny klienta**.
2. W nowo otwartym oknie dialogowym zaznacz Wygasa: **Nigdy** i kliknij **Dodaj**.
3. Sprawdź klucz tajny aplikacji w polu **Wartość** i koniecznie go zapamiętaj.



Więcej informacji na temat klucza tajnego aplikacji można znaleźć w dokumentacji firmy Microsoft.

Zmienianie poświadczeń dostępu do usługi Microsoft 365

Poświadczenia dostępu do usługi Microsoft 365 można zmienić bez ponownego instalowania agenta.

Aby zmienić poświadczenia dostępu do usługi Microsoft 365

1. W konsoli internetowej Cyber Protect przejdź do sekcji **Urządzenia** > **Microsoft Office 365**.
2. Wybierz organizację Microsoft 365.
3. Kliknij **Określ poświadczenia**.
4. Wprowadź identyfikator i klucz tajny aplikacji oraz identyfikator dzierżawcy Microsoft 365. Więcej informacji na temat ich lokalizacji można znaleźć w sekcji Uzyskiwanie identyfikatora i klucza tajnego aplikacji.
5. Kliknij **Zaloguj się**.

Wybór skrzynek pocztowych

Wybierz skrzynki pocztowe zgodnie z poniższym opisem, a następnie odpowiednio określ inne ustawienia planu ochrony.

Aby wybrać skrzynki pocztowe

1. W konsoli internetowej Cyber Protect przejdź do sekcji **Urządzenia** > **Microsoft Office 365**.
2. Wybierz skrzynki pocztowe, które chcesz uwzględnić w kopii zapasowej.
3. Kliknij **Kopia zapasowa**.

Odzyskiwanie skrzynek pocztowych i elementów skrzynek pocztowych

Odzyskiwanie skrzynek pocztowych

1. [Tylko w przypadku odzyskiwania na serwer Exchange Server] Sprawdź, czy istnieje użytkownik programu Exchange z tą samą nazwą logowania co nazwa użytkownika odzyskiwanej skrzynki pocztowej. Jeśli nie, utwórz takiego użytkownika. Zobacz pełną listę wymagań dotyczących tego użytkownika w sekcji "Wymagania dotyczące kont użytkowników" (s. 477).
2. W konsoli internetowej Cyber Protect przejdź do sekcji **Urządzenia** > **Microsoft Office 365**.
3. 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, zaznacz ją na karcie Magazyn kopii zapasowych, a następnie kliknij **Pokaż kopie zapasowe**.
4. Wybierz punkt odzyskiwania. Uwaga, punkty odzyskiwania są filtrowane na podstawie lokalizacji.
5. Kliknij **Odzyskaj** > **Skrzynka pocztowa**.
6. Aby odzyskać dane na serwer programu Exchange, w polu **Odzyskaj do** wybierz pozycję **Microsoft Exchange**. Kontynuuj odzyskiwanie zgodnie z opisem podanym w sekcji "Odzyskiwanie skrzynek pocztowych" (s. 478), rozpoczynając od kroku 9. Kolejne kroki tej procedury nie są wymagane.
   Aby odzyskać dane do usługi Microsoft 365, w polu **Odzyskaj do** zachowaj wartość domyślną **Microsoft Office 365**.
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**.

Odzyskiwanie elementów skrzynki pocztowej

1. [Tylko w przypadku odzyskiwania na serwer Exchange Server] Sprawdź, czy istnieje użytkownik programu Exchange z tą samą nazwą logowania co nazwa użytkownika odzyskiwanej skrzynki pocztowej. Jeśli nie, utwórz takiego użytkownika. Zobacz pełną listę wymagań dotyczących tego użytkownika w sekcji "Wymagania dotyczące kont użytkowników" (s. 477).
2. W konsoli internetowej Cyber Protect przejdź do sekcji **Urządzenia** > **Microsoft Office 365**.
3. 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, zaznacz ją na karcie Magazyn kopii zapasowych, a następnie kliknij **Pokaż kopie zapasowe**.

4. Wybierz punkt odzyskiwania. Uwaga, punkty odzyskiwania są filtrowane na podstawie lokalizacji.
5. Kliknij **Odzyskaj** > **Wiadomości e-mail**.
6. 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.

   Uwaga
   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”: 
7. Kliknij **Odzyskaj**.
8. Aby odzyskać dane na serwer programu Exchange, w polu **Odzyskaj do** wybierz pozycję **Microsoft Exchange**.

   Aby odzyskać dane do usługi Microsoft 365, w polu **Odzyskaj do** zachowaj wartość domyślną **Microsoft Office 365**.
9. [Tylko w przypadku odzyskiwania na serwer programu Exchange] Aby wybrać lub zmienić komputer docelowy, kliknij **Komputer docelowy z programem Microsoft Exchange Server**. 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, określ poświadczenia konta, które będzie używane w celu uzyskania dostępu do komputera. Wymagania dotyczące takiego konta można znaleźć w sekcji "Wymagane prawa użytkownika" (s. 469).
10. 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.
11. [Tylko w przypadku odzyskiwania wiadomości e-mail] W polu **Folder docelowy** wyświetl lub zmień folder docelowy w docelowej skrzynce pocztowej. Domyślnie wybrany jest folder **Odzyskane elementy**.
12. Kliknij **Rozpocznij odzyskiwanie**.

Ochrona danych z Google Workspace

Ta funkcja jest dostępna tylko w chmurowych wdrożeniach programu Acronis Cyber Protect. Szczegółowy opis tej funkcji można znaleźć na stronie https://www.acronis.com/support/documentation/CyberProtectionService/#protecting-google-workspace-data.html.

Ochrona systemu Oracle Database

Metody ochrony systemu Oracle Database opisano w osobnym dokumencie dostępnym pod adresem https://dl.managed-protection.com/u/pdf/AcronisCyberProtect_15_OracleBackup_whitepaper.pdf

Specjalne operacje dotyczące maszyn wirtualnych

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 przywracaniem 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**
  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

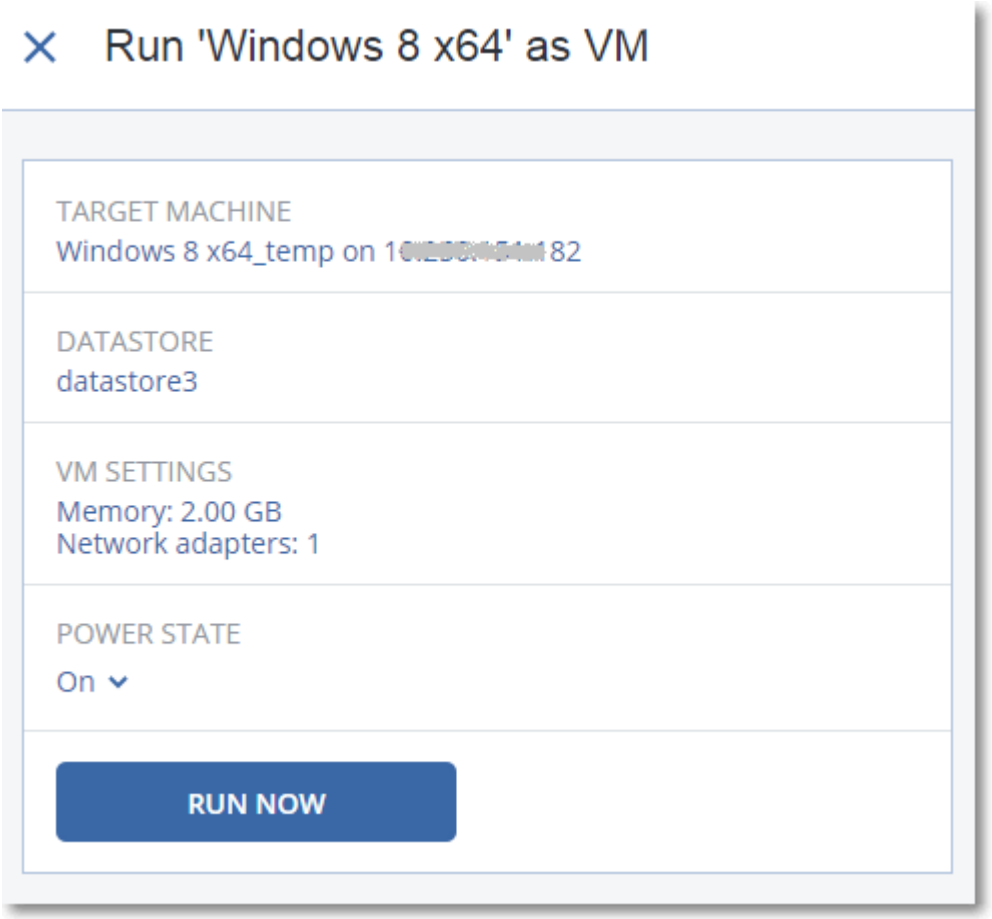
- W usłudze Cyber Protection musi być zarejestrowany co najmniej jeden agent dla VMware lub agent dla Hyper-V.
- Kopia zapasowa może być przechowywana w folderze sieciowym, węźle magazynowania lub folderze lokalnym komputera z zainstalowanym agentem dla VMware lub agentem dla Hyper-V. Jeśli wybierzesz 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. Nie można uruchomić maszyny wirtualnej z poziomu kopii zapasowej przechowywanej na serwerze SFTP, urządzeniu taśmowym lub partycji Secure Zone.

- 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.
- Kopie zapasowe zawierające woluminy logiczne systemu Linux (LVM) muszą zostać utworzone przez agenta dla VMware lub agenta dla Hyper-V. Maszyna wirtualna musi być tego samego typu co pierwotna maszyna (ESXi lub Hyper-V).

Uruchamianie maszyny

1. Wykonaj jedną z następujących czynności:
   - Wybierz komputer uwzględniony w kopii zapasowej, kliknij **Odzyskaj**, a następnie wybierz punkt odzyskiwania.
   - Wybierz punkt odzyskiwania na karcie Magazyn kopii zapasowych.
2. Kliknij **Uruchom jako maszynę wirtualną**.
   Program automatycznie wybierze host i inne wymagane parametry.



3. [Opcjonalnie] Kliknij **Komputer docelowy**, a następnie zmień typ maszyny wirtualnej (ESXi lub Hyper-V), host lub nazwę maszyny wirtualnej.

4. [Opcjonalnie] Kliknij **Magazyn danych** w przypadku maszyny ESXi lub **Ścieżka** w przypadku maszyny 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. Jeśli zamierzasz zachować te zmiany przez skonfigurowanie maszyny wirtualnej jako trwałej, wybierz magazyn danych nadający się do obsługi tej maszyny w środowisku produkcyjnym.
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 wyniku tego maszyna będzie pokazywana w interfejsie internetowym z jedną z następujących ikon:  lub 

. Takich maszyn wirtualnych nie można wybierać do uwzględnienia w kopii zapasowej.

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.

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 ochrony maszyna może przestać być dostępna lub nawet zostać uszkodzona.

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 trakcie finalizacji.

Lokalizacja finalnych dysków wirtualnych jest określona w parametrach operacji **Uruchom jako maszynę wirtualną** (**Magazyn danych** w przypadku ESXi lub **Ścieżka** w przypadku Hyper-V). Przed rozpoczęciem finalizacji należy się upewnić, że wolne miejsce, możliwości udostępniania i wydajność magazynu danych są wystarczające, aby uruchomić maszynę w środowisku produkcyjnym.

Uwaga
Finalizacja nie jest obsługiwana w przypadku funkcji Hyper-V działającego w systemach Windows Server 2008/2008 R2 i Microsoft Hyper-V Server 2008/2008 R2, ponieważ w tych wersjach funkcji Hyper-V brakuje niezbędnego interfejsu API.

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**.
5. Kliknij **Finalizuj**.

Nazwa maszyny zostanie natychmiast zmieniona. Na karcie **Działania** jest wyświetlany postęp odzyskiwania.Po ukończeniu odzyskiwania ikona maszyny zostanie zastąpiona ikoną zwykłej maszyny wirtualnej.

Co trzeba wiedzieć o finalizacji

Finalizacja a zwykłe odzyskiwanie

Proces finalizacji zajmuje więcej czasu niż zwykłe odzyskiwanie z następujących powodów:

- Podczas finalizacji agent losowo uzyskuje dostęp do różnych części kopii zapasowej. W przypadku odzyskiwania całej maszyny agent sekwencyjnie odczytuje dane z kopii zapasowej.
- Jeśli maszyna wirtualna działa podczas finalizacji, agent częściej odczytuje dane z kopii zapasowej, aby podtrzymać jednoczesne działanie obu procesów. Podczas zwykłego odzyskiwania maszyna wirtualna zostaje zatrzymana.

Finalizacja maszyn uruchomionych z kopii zapasowych w chmurze

Ze względu na intensywność uzyskiwania dostępu do danych kopii zapasowych szybkość finalizacji w dużym stopniu zależy od przepustowości łącza między lokalizacją kopii zapasowych a agentem. W przypadku kopii zapasowych znajdujących się w chmurze finalizacja zajmie więcej czasu niż w przypadku lokalnych kopii zapasowych. Jeśli połączenie z Internetem jest bardzo wolne lub niestabilne, finalizacja maszyny uruchomionej z kopii zapasowej w chmurze może się nie udać. Jeśli planujesz finalizację i masz wybór, najlepiej uruchom maszyny wirtualne z lokalnych kopii zapasowych.

Praca w środowisku VMware vSphere

W tej sekcji opisano operacje specyficzne dla środowisk VMware vSphere.

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, 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**
  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**

  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 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

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 oryginalnego 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.
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: 

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.

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 pole wyboru **Zatrzymaj oryginalną maszynę wirtualną**, aby utrzymać oryginalną maszynę w trybie online.
6. Kliknij **Rozpocznij**.

Gdy replika jest w stanie przełączania awaryjnego, możesz wybrać jedną z następujących czynności:

- **Zatrzymaj przełączanie awaryjne**

  Zatrzymaj przełączanie awaryjne, jeśli pierwotna maszyna została naprawiona. Replika zostanie wyłączona. Nastąpi wznowienie replikacji.
- **Wykonaj trwałe przełączenie awaryjne na replikę**

  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**

  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.

Zatrzymywanie przełączenia 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.

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**.

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.
7. Kliknij **Rozpocznij odzyskiwanie**.
8. Potwierdź decyzję.

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)".

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".

Polecenia poprzedzające/następujące

Ta opcja jest podobna do opcji tworzenia kopii zapasowych „Polecenia poprzedzające/następujące".

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".

Opcje powrotu po awarii

Aby zmodyfikować opcje powrotu po awarii, kliknij **Opcje odzyskiwania** podczas konfigurowania powrotu po awarii.

Obsługa błędów

Opcja ta jest podobna do opcji odzyskiwania „Obsługa błędów".

Wydajność

Opcja jest podobna do opcji odzyskiwania „Wydajność".

Polecenia poprzedzające/następujące

Opcja ta jest podobna do opcji odzyskiwania „Polecenia poprzedzające/następujące".

Zarządzanie zasilaniem maszyn wirtualnych

Opcja ta jest podobna do opcji odzyskiwania „Zarządzanie zasilaniem maszyn wirtualnych".

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.
   - Jeśli pierwotna maszyna wirtualna nie może zostać wyłączona, przejdź do następnego kroku.
2. Utwórz plan replikacji.

   Podczas tworzenia planu w polu **Komputer docelowy** wybierz **Nowa replika** oraz host ESXi, na którym znajduje się oryginalna maszyna.
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.

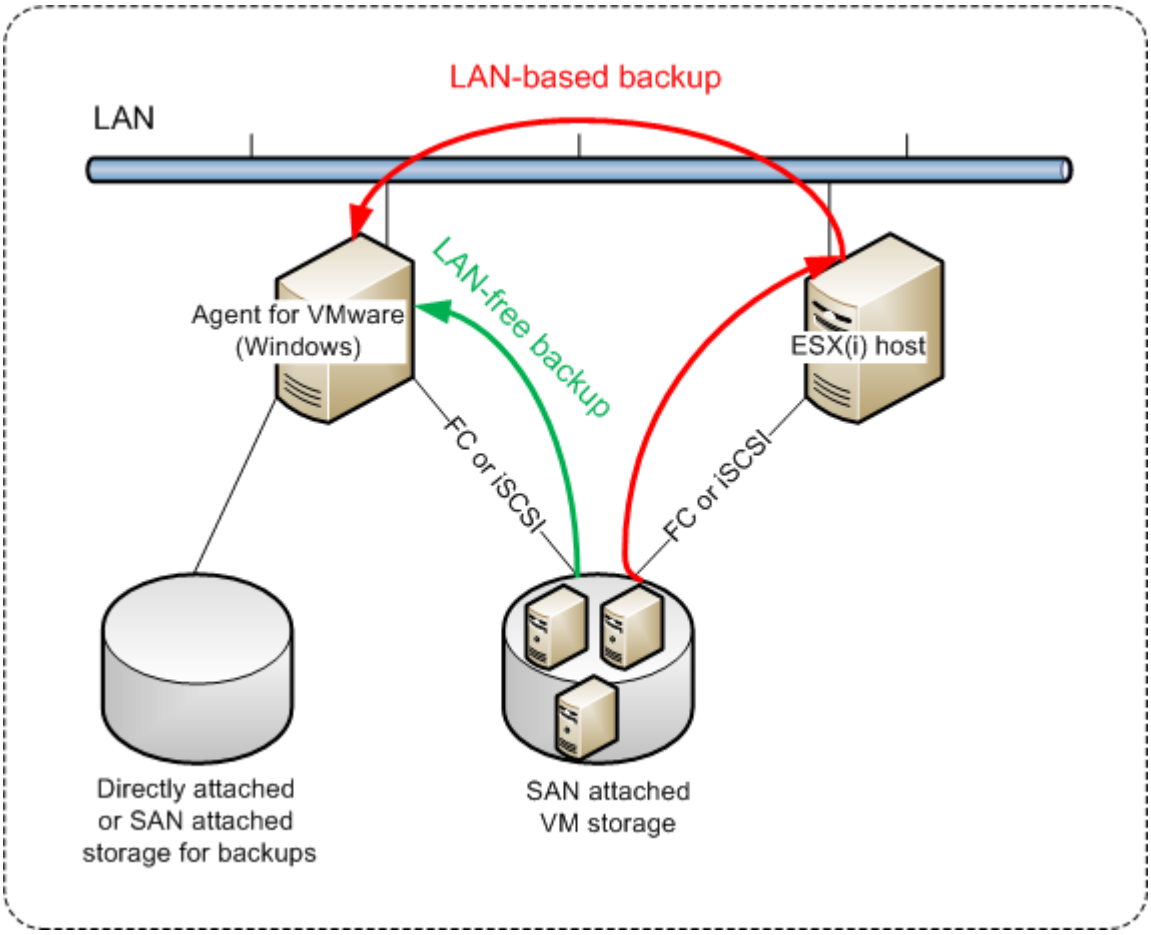
W wyniku tych działań oprogramowanie będzie nadal aktualizować replikę. Wszystkie replikacje będą przyrostowe.

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.

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.

     Aby uniknąć inicjowania jednostki LUN, **Zasady sieci SAN** są automatycznie ustawiane na **Wszystkie offline** podczas instalacji agenta dla VMware (Windows).

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 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 skonfigurować zasady SAN

1. Zaloguj się jako administrator, otwórz wiersz polecenia, wpisz `diskpart`, a następnie naciśnij **Enter**.
2. Wpisz `san`, a następnie naciśnij **Enter**. Upewnij się, że jest wyświetlana opcja **Zasady SAN: Wszystkie offline**.
3. Jeśli jest ustawiona inna wartość zasad SAN:
   a. Wpisz `san policy=offlineall`.
   b. Naciśnij **Enter**.
   c. Aby sprawdzić, czy ustawienia zostały poprawnie zastosowane, wykonaj krok 2.
   d. Uruchom ponownie komputer.

Aby skonfigurować inicjator iSCSI

1. Przejdź do sekcji **Panel sterowania** > **Narzędzia administracyjne** > **Inicjator iSCSI**.

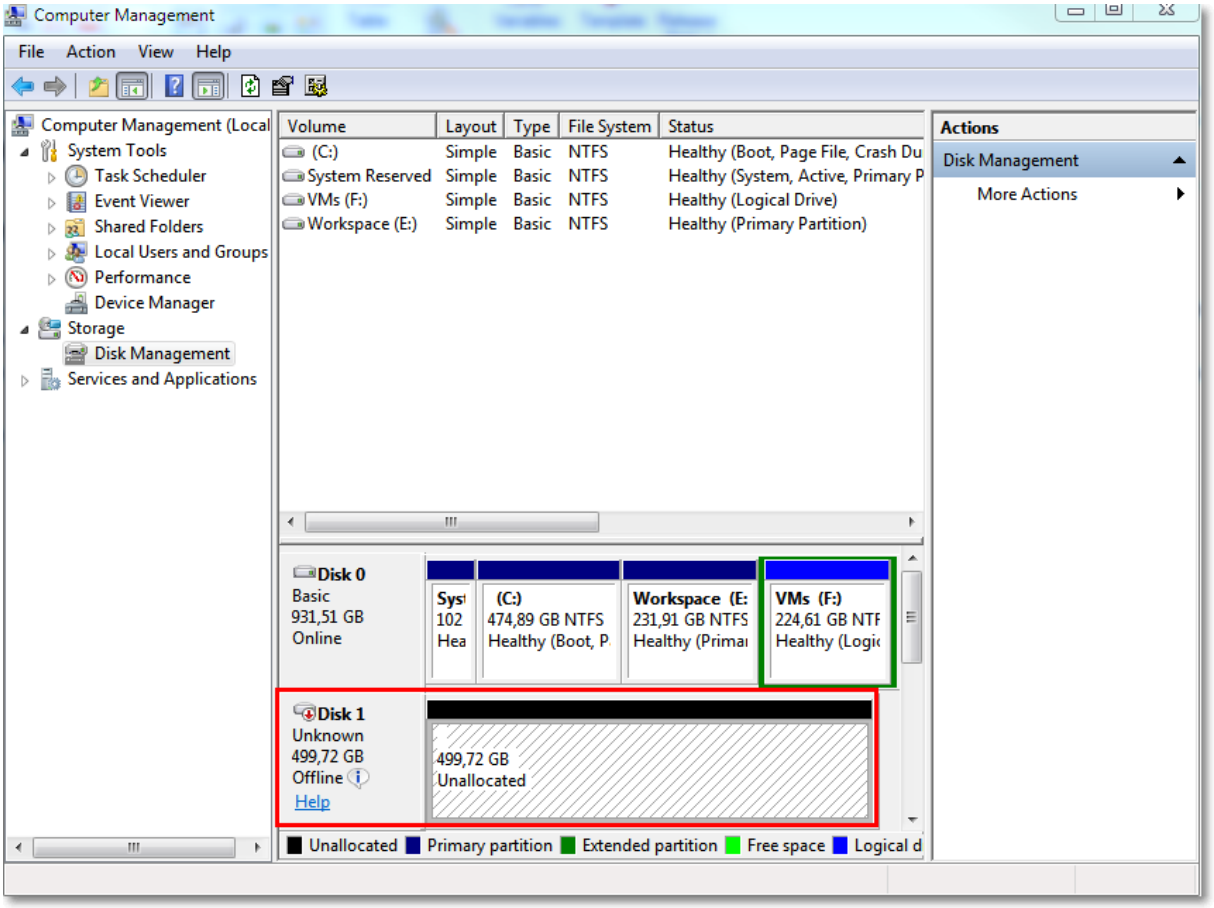
   Uwaga
   Aby znaleźć aplet **Narzędzia administracyjne**, być może trzeba będzie zmienić widok w **Panelu sterowania** na inny niż **Narzędzia główne** czy **Kategoria** albo skorzystać z funkcji wyszukiwania.

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**.

Gotowa jednostka LUN sieci SAN powinna się pojawić w obszarze **Zarządzanie dyskami**, tak jak pokazano na poniższym zarzucie ekranu.



Korzystanie z migawek urządzeń SAN

Jeśli magazyn danych programu VMware vSphere jest oparty na systemie magazynów w sieci SAN, można włączyć agenta dla VMware (Windows), aby używać migawek urządzeń SAN podczas tworzenia kopii zapasowych.

Ważne
Jest obsługiwany tylko magazyn SAN NetApp.

Dlaczego należy używać migawek urządzeń SAN?

Agent dla VMware wymaga migawki maszyny wirtualnej do utworzenia spójnej kopii zapasowej. Agent odczytuje zawartość dysku wirtualnego z migawki, dlatego migawka musi zostać zachowana przez cały proces tworzenia kopii zapasowej.

Domyślnie agent korzysta z migawek VMware, które tworzy host ESXi. W czasie, kiedy migawka jest zachowywana, pliki na dysku wirtualnym są w stanie tylko do odczytu, a host zapisuje wszystkie zmiany wprowadzone na dysku w oddzielnych plikach różnicowych. Po ukończeniu tworzenia kopii zapasowej host usuwa migawkę — scala pliki różnicowe z plikami na dysku wirtualnym.

Zachowywanie i usuwanie migawek wpływa na wydajność maszyny wirtualnej. W przypadku dużych dysków wirtualnych i szybkich zmian danych te operacje mogą być czasochłonne i powodować zmniejszenie wydajności. W ekstremalnych sytuacjach, w których jednocześnie są tworzone kopie zapasowe wielu komputerów, rosnące pliki różnicowe mogą prawie zapełnić magazyn danych i spowodować wyłączenie wszystkich maszyn wirtualnych.

Aby obniżyć użycie zasobów przez hiperwizora, można przenieść migawki do sieci SAN. W takim przypadku następuje poniższa sekwencja operacji:

1. Serwer ESXi tworzy migawkę VMware na początku procesu tworzenia kopii zapasowej, aby wymusić spójny stan dysków wirtualnych.
2. Sieć SAN tworzy migawkę urządzenia woluminu lub jednostki LUN, która zawiera maszynę wirtualną i jej migawkę VMware. Ta operacja zazwyczaj trwa kilka sekund.
3. Serwer ESXi usuwa migawkę VMware. Agent dla VMware odczytuje zawartość dysku wirtualnego z migawki urządzenia SAN.

Migawka VMware jest zachowywana tylko przez kilka sekund, co redukuje wpływ na wydajność maszyny wirtualnej.

Co jest potrzebne do używania migawek urządzenia SAN?

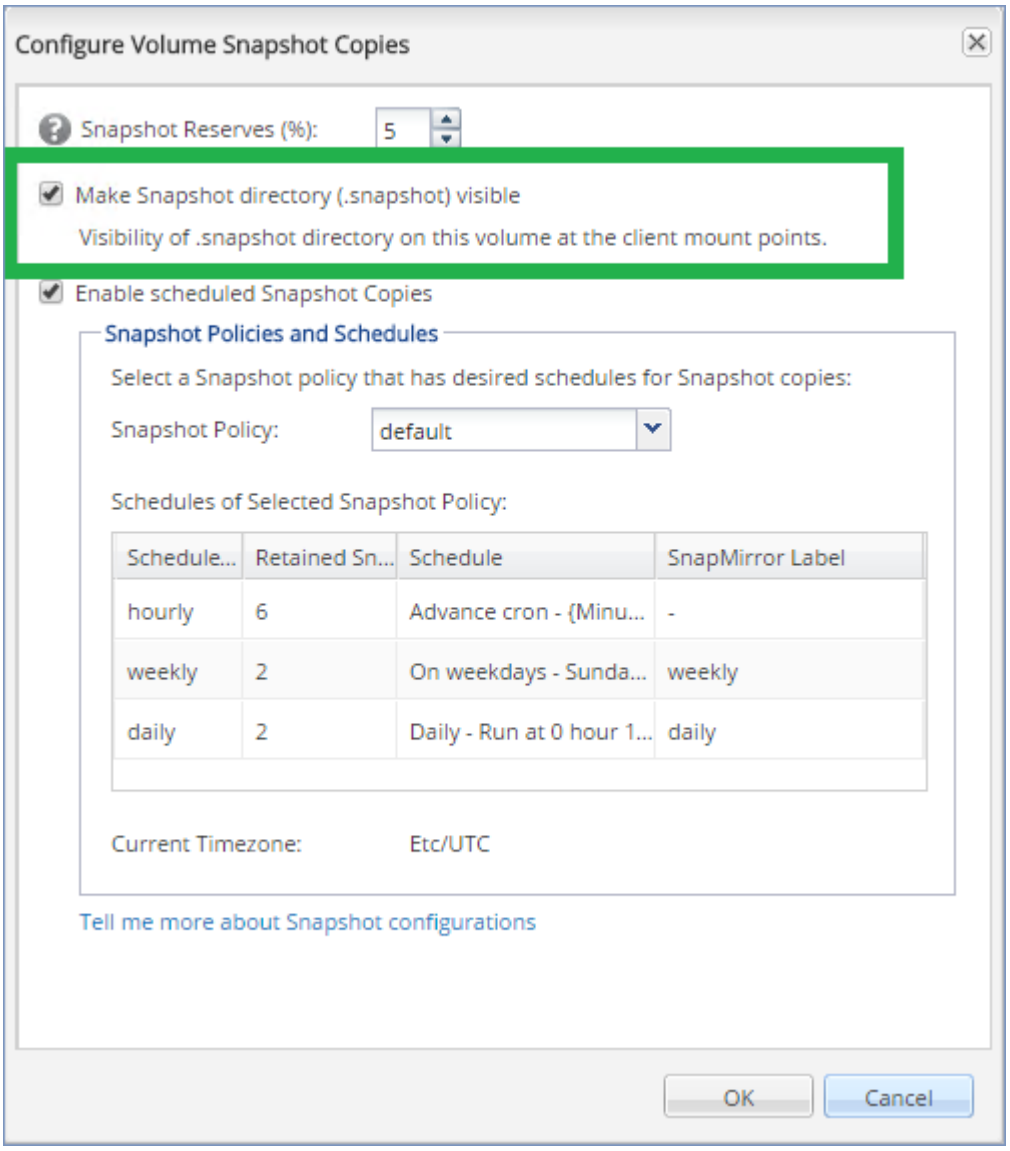
Aby korzystać z migawek urządzenia SAN podczas tworzenia kopii zapasowych maszyn wirtualnych, upewnij się, że są spełnione następujące warunki:

- Magazyn SAN NetApp spełnia wymagania opisane w sekcji Wymagania dotyczące magazynu SAN NetApp.
- Komputer, na którym jest uruchomiony agent dla VMware (Windows), jest skonfigurowany zgodnie z opisem w sekcji Konfigurowanie komputera z uruchomionym agentem dla VMware.
- Magazyn SAN jest zarejestrowany na serwerze zarządzania.
- Jeśli istnieją agenty VMware, które nie uczestniczyły w powyższej rejestracji, maszyny wirtualne znajdujące się w magazynie SAN są przypisywane do agentów obsługujących sieć SAN zgodnie z opisem Wiązanie maszyn wirtualnych.
- Opcja tworzenia kopii zapasowych Migawki urządzenia SAN jest włączona w opcjach planu ochrony.

Wymagania dotyczące magazynu SAN NetApp

- Magazyn SAN musi być użyty jako magazyn danych NFS lub iSCSI.
- W magazynie SAN musi być uruchomiony program Data ONTAP 8.1 lub nowszy w trybie **Clustered Data ONTAP (cDOT)**. Tryb **7-mode** nie jest obsługiwany.

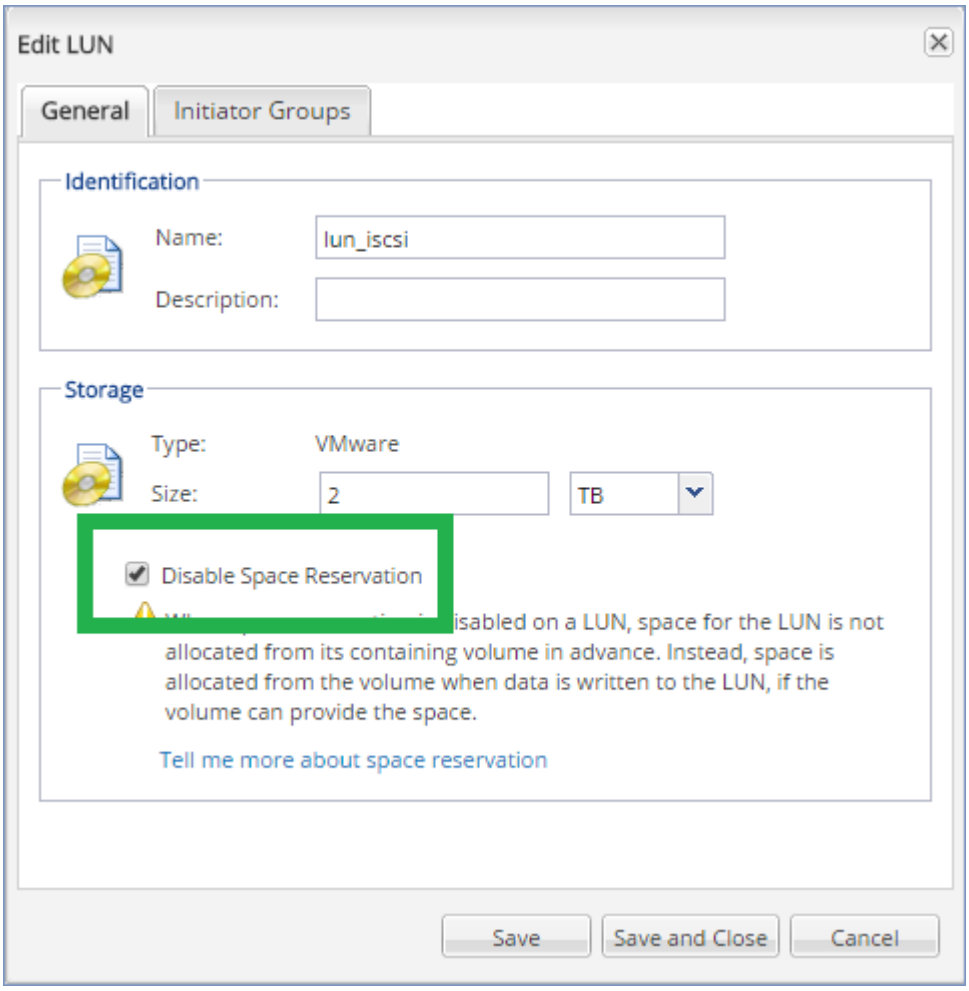
- W programie NetApp OnCommand System Manager należy zaznaczyć pole wyboru **Kopie migawki** > **Konfiguruj** > **Ustaw katalog migawki (.snapshot) jako widoczny** dla woluminu, w którym znajduje się magazyn danych.



- [W przypadku magazynów danych NFS] Należy włączyć dsotęp do udziałów NFS z klientów NFSv3 systemu Windows w maszynie wirtualnej magazynu (SVM), która została określona podczas tworzenia magazynu danych. Dostęp można włączyć przy użyciu następującego polecenia:

  ```
  vserver nfs modify -vserver [SVM name] -v3-ms-dos-client enable
  ```

  Więcej informacji można znaleźć w dokumencie dotyczącym najlepszych praktyk związanych z NetApp: https://kb.netapp.com/support/s/article/ka21A0000000k89QAA/top-windows-nfsv3-0-issues-workarounds-and-best-practices
- [W przypadku magazynów danych iSCSI] W programie NetApp OnCommand System Manager należy zaznaczyć pole wyboru **Wyłącz rezerwację miejsca** dla jednostki iSCSI LUN, w której znajduje się magazyn danych.



Konfigurowanie komputera z uruchomionym agentem dla VMware

W zależności od tego, czy magazyn SAN jest używany jako magazyn danych NFS, czy też iSCSI zapoznaj się z odpowiednią sekcją poniżej.

Konfigurowanie inicjatora iSCSI

Upewnij się, że są spełnione następujące warunki:

- Jest zainstalowany program Microsoft iSCSI Initiator.
- Typ uruchamiania usługi Microsoft iSCSI Initiator jest ustawiony jako **Automatycznie** lub **Ręcznie**. Można to zrobić w przystawce **Usługi**.
- Inicjator iSCSI jest skonfigurowany zgodnie z opisem w sekcji przykładu „Tworzenie kopii zapasowych bez obciążania sieci lokalnej”.

Konfigurowanie klienta NFS

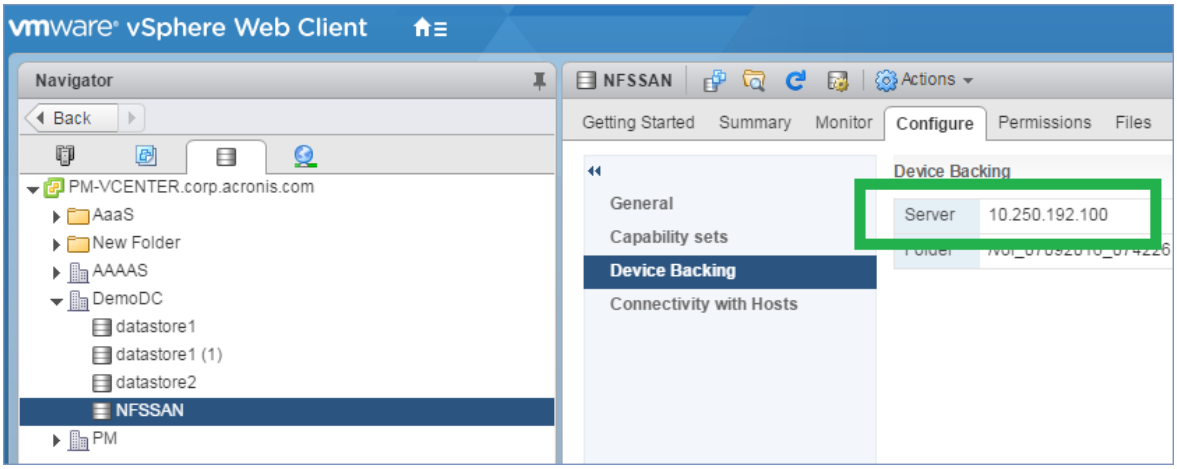
Upewnij się, że są spełnione następujące warunki:

- Są zainstalowane **Usługi firmy Microsoft dla systemu plików NFS** (w systemie Windows Server 2008) lub **Klient systemu plików NFS** (w systemie Windows Server 2012 lub nowszym).

- Klient systemu plików NFS jest skonfigurowany do anonimowego dostępu. Można to zrobić w następujący sposób:
  a. Uruchom Edytor rejestru.
  b. Odszukaj następujący klucz rejestru: **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\ClientForNFS\CurrentVersion\Default**
  c. W tym kluczu utwórz nową wartość **DWORD** o nazwie **AnonymousUID** i ustaw jej dane wartości na 0.
  d. W tym samym kluczu utwórz nową wartość **DWORD** o nazwie **AnonymousGID** i ustaw jej dane wartości na 0.
  e. Uruchom ponownie komputer.

Rejestrowanie magazynu SAN na serwerze zarządzania

1. Kliknij **Ustawienia** > **Magazyn SAN**.
2. Kliknij **Dodaj magazyn**.
3. [Opcjonalnie] W polu **Nazwa** zmień nazwę magazynu.
   Ta nazwa będzie wyświetlana na karcie **Magazyn SAN**.
4. W polu**Nazwa hosta lub adres IP** określ maszynę wirtualną magazynu NetApp (maszynę wirtualną magazynu nazywaną również maszyną wirtualną archiwizacji), którą określono podczas tworzenia magazynu danych.
   Aby znaleźć wymagane informacje w kliencie internetowym VMware vSphere, wybierz magazyn danych, a następnie kliknij **Konfiguruj** > **Tworzenie kopii zapasowej urządzenia**. Nazwa hosta lub adres IP są wyświetlone w polu **Serwer**.



5. W polach **Nazwa użytkownika** i **Hasło** określ poświadczenia administratora maszyny wirtualnej magazynu.

Ważne
Wskazane konto musi mieć prawa administratora lokalnego na maszynie wirtualnej magazynu, a nie administratora zarządzania w kontekście całego systemu NetApp.

Program umożliwia określenie istniejącego użytkownika lub utworzenie nowego użytkownika. Aby utworzyć nowego użytkownika, w programie NetApp OnCommand System Manager przejdź do pozycji **Konfiguracja** > **Zabezpieczenia** > **Użytkownicy**, a następnie utwórz nowego użytkownika.

6. Wybierz co najmniej jednego agenta dla VMware (Windows), który otrzyma uprawnienia odczytu do tego urządzenia SAN.
7. Kliknij **Dodaj**.

Używanie magazynu dołączonego lokalnie

Do agenta dla VMware (urządzenie wirtualne) można dołączyć dodatkowy dysk pełniący funkcję magazynu dołączonego lokalnie, w którym agent może przechowywać kopie zapasowe. Takie rozwiązanie eliminuje ruch sieciowy między agentem a lokalizacją kopii zapasowych.

Urządzenie wirtualne, które działa na tym samym hoście lub w tym samym klastrze co maszyny wirtualne uwzględniane w kopiach zapasowych, ma bezpośredni dostęp do magazynów danych, w których znajdują się te maszyny. Oznacza to, że urządzenie może podłączyć dyski uwzględniane w kopiach zapasowych przy użyciu transportu HotAdd, w związku z czym ruch związany z tworzeniem kopii zapasowych jest kierowany z jednego dysku lokalnego na drugi. Jeśli magazyn danych jest podłączony jako **Dysk/jednostka LUN**, a nie folder **NFS**, operacja tworzenia kopii zapasowej zostanie wykonana bez korzystania z sieci lokalnej. W przypadku magazynu danych NFS wystąpi ruch sieciowy między nim a hostem.

Użycie magazynu dołączonego lokalnie oznacza, że agent będzie zawsze tworzył kopie zapasowe tych samych komputerów. Jeśli w środowisku vSphere jest uruchomionych wiele agentów, a co najmniej jeden z nich używa magazynów dołączonych lokalnie, należy ręcznie powiązać każdego agenta ze wszystkimi komputerami, których kopie zapasowe ma on tworzyć. W innym przypadku, jeśli komputery są rozdzielone pomiędzy agenty przez serwer zarządzania, kopie zapasowe jednego komputera mogą być rozproszone w wielu magazynach.

Program umożliwia dodanie magazynu do już działającego agenta lub wykonanie tego w trakcie wdrażania agenta z szablonu OVF.

Aby dołączyć magazyn do już działającego agenta

1. W widoku inwentaryzacji serwera VMware vSphere kliknij prawym przyciskiem myszy opcję Agent dla VMware (urządzenie wirtualne).
2. Dodaj dysk, edytując ustawienia maszyny wirtualnej. Dysk nie może być mniejszy niż 10 GB.

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

3. Przejdź do konsoli urządzenia wirtualnego. W dolnej części ekranu jest dostępne łącze **Utwórz magazyn**. Jeśli go tam nie ma, kliknij opcję **Odśwież**.

4. Kliknij łącze **Utwórz magazyn**, wybierz dysk i określ jego etykietę. Z powodu ograniczeń systemu plików etykieta może mieć długość maksymalnie 16 znaków.

Aby wybrać magazyn dołączony lokalnie jako miejsce docelowe kopii zapasowej

Podczas tworzenia planu ochrony w sekcji **Miejsce docelowe kopii zapasowej** wybierz opcję **Foldery lokalne**, a następnie wpisz literę magazynu dołączonego lokalnie, na przykład **D:**.

Wiązanie maszyn wirtualnych

Poniższa sekcja wyjaśnia, jak serwer zarządzania organizuje pracę wielu agentów w programie VMware vCenter.

Poniższy algorytm dystrybucji dotyczy zarówno urządzeń wirtualnych, jak i agentów zainstalowanych w systemie Windows.

Algorytm dystrybucji

Maszyny wirtualne są automatycznie równomiernie rozprowadzane między agentami dla VMware. Równomiernie oznacza, że każdy agent obsługuje tę samą liczbę komputerów. Rozmiar powierzchni magazynu zajęty przez maszynę wirtualną nie jest obliczany.

Jednak przy wybieraniu agenta dla maszyny program próbuje optymalizować ogólną wydajność systemu. Program uwzględnia w szczególności lokalizację agenta i maszyny wirtualnej. Preferowany jest agent z tego samego hosta. W przypadku braku agenta na tym samym hoście, wybierany jest agent z tego samego klastra.

Po przypisaniu maszyny wirtualnej do agenta wszystkie kopie zapasowe tej maszyny będą delegowane do tego agenta.

Redystrybucja

Do redystrybucji dochodzi za każdym razem, kiedy załamuje się ustalona równowaga, a dokładniej, kiedy nierównowaga obciążenia między agentami przekracza 20 procent. Taka sytuacja może mieć miejsce w przypadku dodania lub usunięcia komputera albo agenta, migracji komputera do innego hosta lub klastra, lub w przypadku ręcznego powiązania komputera z agentem. W takim przypadku serwer zarządzania ponownie odpowiednio przydzieli poszczególne komputery według istniejącego algorytmu.

Przykład: zauważasz potrzebę podłączenia większej liczby agentów w celu zwiększenia przepustowości i wdrażasz w klastrze dodatkowe urządzenie wirtualne. Serwer zarządzania przypisze najbardziej odpowiednie maszyny nowemu agentowi. Zmniejszy się obciążenie starszych agentów.

W przypadku usunięcia agenta z serwera zarządzania komputery przypisane temu agentowi zostaną przydzielone pozostałym agentom. Nie dochodzi do tego jednak w przypadku uszkodzenia agenta lub jego ręcznego usunięcia z systemu vSphere. Proces redystrybucji rozpocznie się dopiero po usunięciu takiego agenta z interfejsu internetowego.

Obserwacja wyniku redystrybucji

Można sprawdzić wynik automatycznej dystrybucji:

- w kolumnie **Agent** dla każdej maszyny wirtualnej w sekcji **Wszystkie urządzenia**;
- w sekcji **Przypisane maszyny wirtualne** panelu **Szczegóły**, kiedy agent jest wybrany w sekcji **Ustawienia** > **Agenci**

Powiązanie ręczne

Powiązanie agenta dla VMware umożliwia wykluczenie maszyny wirtualnej z tego procesu rozdzielania przez określenie agenta, który musi zawsze wykonywać kopie zapasowe tej maszyny. Jest zachowywana ogólna równowaga, ale dana maszyna może zostać przekazana do innego agenta tylko pod warunkiem, że pierwotny agent zostanie usunięty.

Aby powiązać maszynę z agentem

1. Wybierz maszynę.
2. Kliknij opcję **Szczegóły**.
   W sekcji **Przypisany agent** program wyświetla agenta zarządzającego obecnie wybraną maszyną.
3. Kliknij przycisk **Zmień**.
4. Wybierz opcję **Ręcznie**.
5. Wybierz agenta, z którym chcesz powiązać maszynę.
6. Kliknij **Zapisz**.

Aby usunąć powiązanie maszyny z agentem

1. Wybierz maszynę.
2. Kliknij opcję **Szczegóły**.
   W sekcji **Przypisany agent** program wyświetla agenta zarządzającego obecnie wybraną maszyną.
3. Kliknij przycisk **Zmień**.
4. Wybierz opcję **Automatycznie**.
5. Kliknij **Zapisz**.

Wyłączanie automatycznego przypisywania do agenta

Można wyłączyć automatyczne przypisywanie do agenta dla VMware, aby wykluczyć go z procesu dystrybucji. W tym celu należy określić listę maszyn, których kopie zapasowe musi wykonywać ten agent. Zostanie zachowana ogólna równowaga między agentami.

Nie można wyłączyć automatycznego przypisywania do agenta, jeśli nie ma innych zarejestrowanych agentów lub wyłączono automatyczne przypisywanie do wszystkich pozostałych agentów.

Aby wyłączyć automatyczne przypisywanie do agenta

1. Kliknij **Ustawienia** > **Agenty**.
2. Wybierz agenta dla VMware, w przypadku którego chcesz wyłączyć automatyczne przypisywanie.
3. Kliknij opcję **Szczegóły**.
4. Wyłącz przełącznik **Przypisanie automatyczne**.

Przykłady użycia

- Ręczne powiązanie jest przydatne, kiedy trzeba uwzględnić konkretną (bardzo dużą) maszynę podczas tworzenia kopii zapasowych przez agenta dla VMware (Windows) za pośrednictwem łącza Fibre Channel, podczas gdy pozostałe maszyny mają być uwzględniane w tworzeniu kopii przez urządzenia wirtualne.
- Ręczne powiazanie jest konieczne w przypadku używania migawek urządzeń SAN. Powoduje powiązanie agenta dla VMware (Windows), dla którego skonfigurowano migawki urządzeń SAN powiązane z maszynami znajdującymi się w magazynie danych SAN.
- Jeśli agent ma magazyn dołączony lokalnie, należy powiązać maszyny wirtualne z agentem.
- Wyłączenie automatycznego przypisywania umożliwia zagwarantowanie przewidywalnego tworzenia kopii zapasowych konkretnej maszyny zgodnie z określonym harmonogramem. W zaplanowanym czasie agent tworzący kopie zapasowe tylko jednej maszyny wirtualnej nie może być zajęty tworzeniem kopii zapasowych innych maszyn wirtualnych.
- Wyłączenie automatycznego przypisywania jest przydatne, kiedy istnieje wiele hostów ESXi w różnych lokalizacjach geograficznych. Jeśli automatyczne przypisywanie zostanie wyłączone, a maszyny wirtualne z poszczególnych hostów zostaną powiązane z agentami uruchomionymi na tych samych hostach, można zagwarantować, że agent nigdy nie będzie tworzyć kopii zapasowych maszyn uruchomionych na zdalnych hostach ESXi. Pozwoli to ograniczyć ruch sieciowy.

Obsługa migracji maszyn wirtualnych

W tej sekcji opisano, czego należy się spodziewać w przypadku migracji maszyn wirtualnych w środowisku vSphere, w tym migracji między hostami ESXi wchodzącymi w skład klastra vSphere.

Narzędzie vMotion

Narzędzie vMotion umożliwia przeniesienie stanu i konfiguracji maszyny wirtualnej na inny host, podczas gdy dyski maszyny pozostają w tej samej lokalizacji w magazynie współużytkowanym.

- Narzędzie vMotion agenta dla VMware (urządzenie wirtualne) nie jest obsługiwane i jest wyłączone.
- Narzędzie vMotion maszyny wirtualnej jest wyłączone podczas tworzenia kopii zapasowej. Po migracji operacje tworzenia kopii zapasowych nadal będą wykonywane.

Narzędzie Storage VMotion

Narzędzie Storage vMotion umożliwia przenoszenie dysków maszyny wirtualnej z jednego magazynu danych do drugiego.

- Narzędzie Storage vMotion agenta dla VMware (urządzenie wirtualne) nie jest obsługiwane i jest wyłączone.
- Narzędzie Storage vMotion maszyny wirtualnej jest wyłączone podczas tworzenia kopii zapasowej. Po migracji operacje tworzenia kopii zapasowych nadal będą uruchamiane.

Zarządzanie środowiskami wirtualizacji

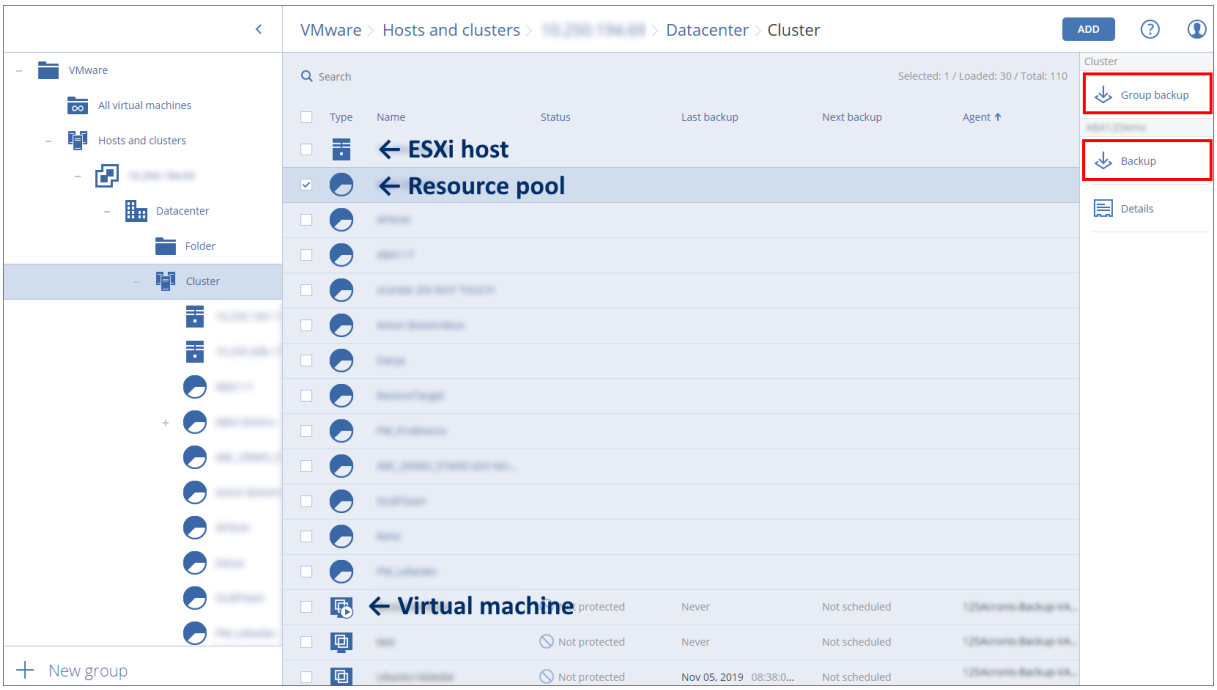
Środowiska vSphere, Hyper-V i Virtuozzo można oglądać w ich macierzystej postaci. Gdy zostanie zainstalowany i zarejestrowany odpowiedni agent, w obszarze **Urządzenia** pojawi się karta **VMware**, **Hyper-V** lub **Virtuozzo**.

Na karcie **VMware** można tworzyć kopie zapasowe następujących obiektów infrastruktury vSphere:

- Centrum danych
- Folder
- Klaster
- Host ESXi
- Pula zasobów

Każdy z tych obiektów infrastruktury działa jako obiekt grupy dla maszyn wirtualnych. W przypadku zastosowania planu ochrony do któregokolwiek z tych obiektów grupy zostanie utworzona kopia zapasowa wszystkich zawartych w nim maszyn wirtualnych. Aby utworzyć kopię zapasową wybranych maszyn grupy, kliknij **Kopia zapasowa** lub zaznacz nadrzędną grupę maszyn wybranej grupy i kliknij **Kopia zapasowa grupy**.

Na przykład załóżmy, że wybrano klaster, a następnie zawartą w nim pulę zasobów. Jeśli klikniesz **Kopia zapasowa**, zostanie utworzona kopia zapasowa wszystkich maszyn wirtualnych w wybranej puli zasobów. Jeśli klikniesz **Kopia zapasowa grupy**, zostanie utworzona kopia zapasowa wszystkich maszyn wirtualnych w klastrze.



Możesz zmienić poświadczenia dostępu do 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 opcję **Szczegóły**.
5. W obszarze **Poświadczenia** kliknij nazwę użytkownika.
6. Określ nowe poświadczenia dostępu, a następnie kliknij **OK**.

Wyświetlanie statusu kopii zapasowej w kliencie vSphere

W kliencie vSphere można wyświetlić status kopii zapasowej i czas utworzenia ostatniej kopii zapasowej maszyny wirtualnej.

Informacje te są wyświetlane w podsumowaniu maszyny wirtualnej (**Podsumowanie** > **Atrybuty niestandardowe** / **Adnotacje** / **Uwagi**, w zależności od typu klienta i wersji środowiska vSphere). Można również włączyć kolumny **Ostatnia kopia zapasowa** i **Status kopii zapasowej** na karcie **Maszyny wirtualne** w przypadku dowolnego hosta, centrum danych, folderu, puli zasobów lub całego serwera vCenter.

Aby można było podać te atrybuty, agent dla VMware musi mieć następujące uprawnienia — oprócz tych opisanych w sekcji „Agent dla VMware — niezbędne uprawnienia”:

- **Globalne** > **Zarządzaj atrybutami niestandardowymi**
- **Globalne** > **Ustaw atrybut niestandardowy**

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.

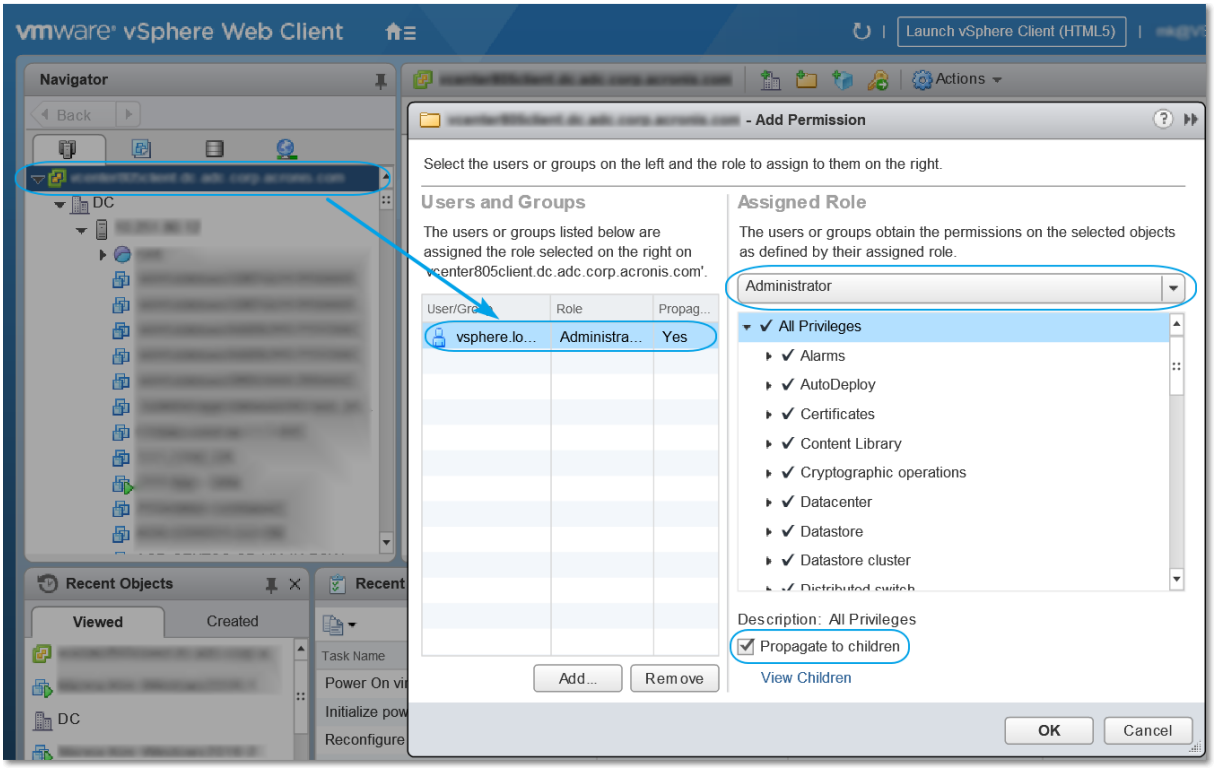
Uwaga
Interfejsy vStorage API muszą być zainstalowane na hoście ESXi, aby można było tworzyć kopie zapasowe maszyn wirtualnych. Zobacz https://kb.acronis.com/content/14931.

W celu wykonania jakiejkolwiek operacji w odniesieniu do obiektów vCenter, takich jak maszyny wirtualne, hosty ESXi, klastry, serwery vCenter i inne, agent dla VMware uwierzytelnia się na serwerze vCenter lub hoście ESXi przy użyciu podanych przez użytkownika poświadczeń vSphere. Konto vSphere, używane przez agenta dla VMware do nawiązania połączenia z vSphere, musi mieć wymagane uprawnienia na wszystkich poziomach infrastruktury vSphere, począwszy od poziomu serwera vCenter.

Podczas instalacji lub konfiguracji agenta dla VMware określ konto vSphere z niezbędnymi uprawnieniami. W razie późniejszej konieczności zmiany konta zajrzyj do sekcji „Zarządzanie środowiskami wirtualizacji”.

Aby przypisać uprawnienia użytkownikowi vSphere na poziomie serwera vCenter:

1. Zaloguj się do klienta internetowego vSphere.
2. Kliknij prawym przyciskiem myszy serwer vCenter, a następnie kliknij **Dodaj uprawnienie**.
3. Wybierz lub dodaj nowego użytkownika z wymaganą rolą (rola musi zawierać wszystkie wymagane uprawnienia z poniższej tabeli).
4. Zaznacz opcję **Propaguj na obiekty podrzędne**.



Obiekt	Uprawnienie	Operacja				
		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	+*				
Magazyn danych	**Przydzielenie miejsca**		+	+	+	+
	Przeglądanie magazynu danych				+	+
	Konfigurowanie magazynu danych	+	+	+	+	+

	Niskopoziomowe operacje na plikach				+	+
Globalne	**Licencje**	+	+	+	+	
	Metody wyłączania	+	+	+		
	Metody włączania	+	+	+		
	Zarządzaj atrybutami niestandardowymi	+	+	+		
	Ustaw atrybut niestandardowy	+	+	+		
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					
	Importuj					+
Maszyna wirtualna > **Konfiguracja**	**Dodanie istniejącego dysku**	+	+		+	
	Dodaj nowy dysk		+	+	+	+
	Dodanie lub usunięcie urządzenia		+		+	+
	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	+**				+
	Modyfikacje 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				+	
	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**	+		+	+	+

Maszyna wirtualna > **Zarządzanie migawkami** (środowisko vSphere 6.5 lub nowsze)						
	Usunięcie migawki	+		+	+	+
vApp	**Dodaj maszynę wirtualną**				+	

* To uprawnienie jest wymagane tylko w przypadku tworzenia kopii zapasowej zaszyfrowanych komputerów.

** To uprawnienie jest wymagane tylko w przypadku kopii zapasowych uwzględniających aplikacje.

Tworzenie kopii zapasowych maszyn Hyper-V w klastrach

W przypadku klastrów Hyper-V maszyny wirtualne mogą migrować między węzłami klastra. Aby poprawnie skonfigurować tworzenie kopii zapasowych maszyn Hyper-V w klastrach, postępuj zgodnie z następującymi zaleceniami:

1. Maszyna musi być dostępna do tworzenia kopii zapasowych bez względu na węzeł, do którego migruje. Aby zapewnić agentowi dla Hyper-V dostęp do maszyny znajdującej się w dowolnym węźle, usługa agenta musi być uruchomiona na koncie użytkownika domeny z uprawnieniami administracyjnymi na każdym węźle klastra.
   Zaleca się określenie takiego konta dla usługi agenta podczas instalacji agenta dla Hyper-V.
2. Zainstaluj agenta dla Hyper-V w każdym węźle klastra.
3. Zarejestruj wszystkie agenty na serwerze zarządzania.

Wysoka dostępność odzyskanej maszyny

W przypadku odzyskiwania dysków z kopii zapasowej na już *istniejącą* maszynę wirtualną Hyper-V jej właściwość Wysoka dostępność pozostanie niezmieniona.

W przypadku odzyskania dysków uwzględnionych w kopii zapasowej na *nową* maszynę wirtualną Hyper-V lub konwersji na maszynę wirtualną Hyper-V w ramach planu ochrony wynikowa maszyna nie będzie się charakteryzowała wysoką dostępnością. Będzie ona traktowana jako maszyna zapasowa i będzie normalnie wyłączona. Jeśli wymagane jest użycie maszyny w środowisku produkcyjnym, można skonfigurować jej wysoką dostępność za pomocą przystawki **Zarządzanie klastrem awaryjnym**.

Ograniczanie łącznej liczby maszyn wirtualnych, których kopie zapasowe mogą być tworzone w tym samym czasie

Opcja tworzenia kopii zapasowych **Harmonogram** określa liczbę maszyn wirtualnych, których kopie zapasowe agent może utworzyć jednocześnie podczas wykonywania danego planu ochrony.

Jeśli plany ochrony nakładają się na siebie w czasie, liczby określone w ich opcjach tworzenia kopii zapasowych są sumowane. Nawet jeśli wynikowa liczba łączna jest programowo ograniczona do 10, nakładające się plany mogą mieć wpływ na wydajność tworzenia kopii zapasowych i powodować przeciążenie zarówno hosta, jak i magazynu maszyn wirtualnych.

Łączną liczbę maszyn wirtualnych, których kopie zapasowe może tworzyć agent dla VMware lub agent dla Hyper-V w tym samym czasie, można dodatkowo ograniczyć.

Aby ograniczyć łączną liczbę maszyn wirtualnych, których kopie zapasowe może tworzyć agent dla VMware (Windows) lub agent dla Hyper-V

1. Na komputerze z uruchomionym agentem utwórz nowy dokument tekstowy i otwórz go w edytorze tekstowym, np. w programie Notatnik.
2. Skopiuj i wklej do pliku następujące wiersze:

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_
MACHINE\SOFTWARE\Acronis\MMS\Configuration\ManagedMachine\SimultaneousBackupsLimits]
"MaxNumberOfSimultaneousBackups"=dword:00000001
```

3. Zastąp `00000001` wartością szesnastkową limitu, który chcesz ustawić. Na przykład `00000001` oznacza 1, a `0000000A` oznacza 10.
4. Zapisz dokument pod nazwą **limit.reg**.
5. Uruchom plik jako administrator.
6. Potwierdź, że chcesz edytować rejestr systemu Windows.
7. 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
```

Aby ograniczyć łączną liczbę maszyn wirtualnych, których kopie zapasowe może tworzyć agent dla VMware (urządzenie wirtualne) lub agent VMware (Linux)

1. Na komputerze z uruchomionym agentem uruchom powłokę poleceń:
   - **Agent dla VMware (urządzenie wirtualne):** naciśnij CTRL+SHIFT+F2 w interfejsie użytkownika urządzenia wirtualnego.
   - **Agent dla VMware (Linux):** zaloguj się jako użytkownik root na komputerze z uruchomionym urządzeniem Acronis Cyber Protect. Hasło jest takie samo jak hasło do konsoli internetowej Cyber Protect.
2. Otwórz plik **/etc/Acronis/MMS.config** w edytorze tekstowym, np. programie **vi**.
3. Odszukaj następującą sekcję:

   ```
   <key name="SimultaneousBackupsLimits">
       <value name="MaxNumberOfSimultaneousBackups" type="Tdword">"10"</value>
   </key>
   ```

4. Zastąp `10` wartością dziesiętną limitu, który chcesz ustawić.
5. Zapisz plik.
6. Uruchom ponownie agenta:
   - **Agent dla VMware (urządzenie wirtualne):** wykonaj polecenie `reboot`.
   - **Agent dla VMware (Linux):** wykonaj polecenie

     ```
     sudo service acronis_mms restart
     ```

Migracja komputera

Migracji komputera można dokonać przez odzyskanie jego kopii zapasowej na innym komputerze niż komputer pierwotny.

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**	**Maszyna wirtualna Virtuozzo***	**Kontener Virtuozzo***	**Maszyna wirtualna Virtuozzo Hybrid Infrastructure***	**Maszyna wirtualna Scale Computing HC3**	**Maszyna wirtualna RHV/oVirt***
Komputer fizyczny	+	+	+	-	-	+	+	+
Maszyna wirtualna VMware	+	+	+	-	-	+	+	+

ESXi								
Maszyna wirtualna Hyper-V	+	+	+	-	-	+	+	+
Maszyna wirtualna Virtuozzo*	+	+	+	+	-	+	+	+
Kontener Virtuozzo*	-	-	-	-	+	-	-	-
Maszyna wirtualna Virtuozzo Hybrid Infrastructure*	+	+	+	-	-	+	+	+
Maszyna wirtualna Scale Computing HC3	+	+	+	-	-	+	+	+
Maszyna wirtualna Red Hat Virtualization / oVirt*	+	+	+	-	-	+	+	+

* Dostępne tylko w przypadku wdrożenia chmurowego.

Instrukcje przeprowadzania migracji można znaleźć w następujących sekcjach:

- Komputer fizyczny na maszynę wirtualną (P2V) — "Odzyskiwanie komputera fizycznego na maszynę wirtualną" (s. 326)
- Maszyna wirtualna na maszynę wirtualną (V2V) — "Odzyskiwanie maszyny wirtualnej" (s. 329)
- Maszyna wirtualna na komputer fizyczny (V2P) — "Odzyskiwanie maszyny wirtualnej" (s. 329) lub "Odzyskiwanie dysków i woluminów przy użyciu nośnika startowego" (s. 332)

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:

- Przeprowadzenie migracji komputera fizycznego na maszynę wirtualną i migracji maszyny wirtualnej na komputer fizyczny w przypadku komputera z systemem Linux zawierającego woluminy logiczne (LVM). Aby utworzyć kopię zapasową i nośnik startowy na potrzeby odzyskiwania, należy użyć agenta dla systemu Linux lub nośnika startowego.
- Udostępnienie sterowników do określonego sprzętu, co jest krytyczne z perspektywy możliwości uruchamiania systemu.

Maszyny wirtualne Windows Azure i Amazon EC2

Aby utworzyć kopię zapasową maszyny wirtualnej Windows Azure lub Amazon EC2, zainstaluj na niej agenta ochrony. 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”. 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.
- 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://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-howto-site-to-site-resource-manager-portal

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.

Ochrona platformy SAP HANA

Metody ochrony platformy SAP HANA opisano w osobnym dokumencie dostępnym pod adresem: https://dl.managed-protection.com/u/pdf/AcronisCyberProtect_15_SAP_HANA_whitepaper_en-US.pdf.

Ochrona antywirusowa i ochrona w Internecie

Ochrona antywirusowa w usłudze Cyber Protect zapewnia szereg korzyści:

- Znakomitą ochronę na wszystkich etapach działań: proaktywnym, aktywnym i reaktywnym.
- Cztery technologie zabezpieczeń przed złośliwym oprogramowaniem, aby zapewnić najlepszą w swojej klasie wielowarstwową ochronę.
- Zarządzanie aplikacją Microsoft Security Essentials i programem antywirusowym Windows Defender.

Ochrona przed wirusami i złośliwym oprogramowaniem

Moduł Ochrona przed wirusami i złośliwym oprogramowaniem umożliwia chronienie komputerów z systemem Windows lub macOS przed wszystkimi najnowszymi zagrożeniami związanymi ze złośliwym oprogramowaniem. Warto pamiętać, że funkcja Active Protection, która wchodzi w skład ochrony antywirusowej, nie jest obsługiwana na komputerach z systemem macOS. Zobacz pełną listę obsługiwanych funkcji ochrony antywirusowej: Obsługa funkcji w poszczególnych systemach operacyjnych.

Program Acronis Cyber Protect jest obsługiwany i rejestrowany w Centrum zabezpieczeń systemu Windows.

Jeśli w chwili stosowania modułu Ochrona przed wirusami i złośliwym oprogramowaniem komputer jest już chroniony przez rozwiązanie antywirusowe innej firmy, system generuje alert oraz zatrzymuje ochronę w czasie rzeczywistym, aby zapobiec ewentualnym problemom z kompatybilnością i wydajnością. Aby zapewnić pełną funkcjonalność modułu Ochrona przed wirusami i złośliwym oprogramowaniem programu Acronis Cyber Protect, trzeba wyłączyć lub odinstalować rozwiązanie antywirusowe innej firmy.

Dostępne są dla Ciebie następujące funkcje związane ze złośliwym oprogramowaniem:

- Wykrywanie złośliwego oprogramowania w plikach w trybie ochrony w czasie rzeczywistym i na żądanie (w systemach Windows i MacOS)
- Wykrywanie złośliwych zachowań w procesach (w systemie Windows)
- Blokowanie dostępu do złośliwych adresów URL (w systemie Windows)
- Przenoszenie niebezpiecznych plików do kwarantanny
- Dodawanie zaufanych firmowych aplikacji do białej listy

Moduł Ochrona przed wirusami i złośliwym oprogramowaniem obsługuje dwa rodzaje skanowania:

- Skanowanie w ramach ochrony w czasie rzeczywistym
- Skanowanie antywirusowe na żądanie

Skanowanie w ramach ochrony w czasie rzeczywistym

Funkcja ochrony w czasie rzeczywistym sprawdza wszystkie pliki, które są wykonywane lub otwierane na komputerze, aby zapobiec zagrożeniom związanym ze złośliwym oprogramowaniem.

Możesz wybrać jeden z poniższych typów skanowania:

- Wykrywanie przy dostępie oznacza, że program antywirusowy działa w tle i stale aktywnie skanuje system komputera w poszukiwaniu wirusów oraz innych złośliwych zagrożeń, gdy system jest włączony. Złośliwe oprogramowanie zostanie wykryte zarówno podczas wykonywania pliku, jak i podczas różnych operacji dotyczących pliku, np. otwierania go do odczytu lub edycji.
- Skanowanie przy wykonywaniu oznacza, że skanowane są tylko pliki wykonywalne w chwili ich uruchamiania w celu sprawdzenia, czy nie są zainfekowane i nie spowodują żadnych uszkodzeń komputera ani danych. Kopiowanie zainfekowanego pliku nie zostanie wykryte.

Skanowanie antywirusowe na żądanie

Skanowanie antywirusowe jest przeprowadzane zgodnie z harmonogramem.

Wyniki skanowania antywirusowego można monitorować w widżecie **Pulpit nawigacyjny** > **Przegląd** > Ostatnie objęte wpływem.

Ustawienia modułu Ochrona przed wirusami i złośliwym oprogramowaniem

Więcej informacji na temat tworzenia planu ochrony z wykorzystaniem modułu Ochrona przed wirusami i złośliwym oprogramowaniem można znaleźć w sekcji „Tworzenie planu ochrony".

W przypadku modułu Ochrona przed wirusami i złośliwym oprogramowaniem można określić następujące ustawienia.

Active Protection

Funkcja Active Protection chroni system przed oprogramowaniem ransomware oraz złośliwym oprogramowaniem do cryptominingu. Oprogramowanie ransomware szyfruje pliki i żąda okupu w zamian za klucz szyfrowania. Złośliwe oprogramowanie do cryptominingu wykonuje obliczenia matematyczne w tle, przez co kradnie moc procesora i ruch sieciowy.

W wersjach Cyber Backup programu Acronis Cyber Protect: Active Protection jest osobnym modułem w planie ochrony. Moduł ten można osobno konfigurować i stosować do innych urządzeń lub grup urządzeń. W wersjach Protect programu Acronis Cyber Protect: Active Protection wchodzi w skład modułu Ochrona przed wirusami i złośliwym oprogramowaniem.

Usługa Active Protection jest dostępna dla komputerów z następującymi systemami operacyjnymi:

- Systemy operacyjne na komputerach stacjonarnych: Windows 7 Service Pack 1 lub nowszy
  W przypadku komputerów z systemem Windows 7 dopilnuj, aby była zainstalowana aktualizacja systemu Windows 7 (KB2533623).
- Systemy operacyjne na serwerach: Windows Server 2008 R2 lub nowszy.

Na komputerze musi być zainstalowany agent dla systemu Windows.

Sposób działania

Funkcja Active Protection monitoruje procesy działające na chronionym komputerze. Gdy jakiś zewnętrzny proces próbuje zaszyfrować pliki lub dokonać cryptominingu, funkcja Active Protection generuje alert i podejmuje dodatkowe działania, jeśli zostały one określone w konfiguracji.

Ponadto funkcja Active Protection zapobiega nieuprawnionym zmianom we własnych procesach oprogramowania do tworzenia kopii zapasowych, rekordach rejestru, plikach wykonywalnych i konfiguracyjnych oraz kopiach zapasowych przechowywanych w folderach lokalnych.

Do identyfikacji złośliwych procesów funkcja Active Protection używa heurystyki behawioralnej. Funkcja Active Protection porównuje łańcuch działań wykonanych przez proces z łańcuchami zdarzeń zapisanych w bazie danych wzorców złośliwego zachowania. Takie podejście umożliwia funkcji Active Protection wykrycie nowego złośliwego oprogramowania na podstawie jego typowego zachowania.

Ustawienie domyślne: **Włączono**.

Ustawienia funkcji Active Protection

W obszarze **Działanie po wykryciu** wybierz działanie wykonywane przez oprogramowanie po wykryciu działania oprogramowania wymuszającego okup, a następnie kliknij **Gotowe**.

Można wybrać jedną z następujących opcji:

- **Tylko powiadom**
  Oprogramowanie wygeneruje alert dotyczący procesu.
- **Zatrzymaj proces**
  Oprogramowanie wygeneruje alert i zatrzyma proces.
- **Cofnij przy użyciu pamięci podręcznej**
  Oprogramowanie wygeneruje alert, zatrzyma proces i wycofa zmiany w pliku przy użyciu pamięci podręcznej usługi.

Ustawienie domyślne: **Cofnij przy użyciu pamięci podręcznej**.

Ochrona folderów sieciowych

Opcja **Chroń foldery sieciowe zamapowane jako dyski lokalne** pozwala określić, czy moduł Ochrona przed wirusami i złośliwym oprogramowaniem ma chronić foldery sieciowe zamapowane jako dyski lokalne przed lokalnymi złośliwymi procesami.

Opcja ta dotyczy folderów udostępnianych za pomocą protokołów SMB lub NFS.

Jeśli plik pierwotnie znajdował się na zamapowanym dysku, nie można go zapisać w pierwotnej lokalizacji po wyodrębnieniu z pamięci podręcznej za pomocą opcji **Cofnij przy użyciu pamięci podręcznej**. Zamiast tego plik zostanie zapisany w folderze określonym w ustawieniach tej opcji. Domyślny folder to **C:\ProgramData\Acronis\Restored Network Files**. Jeśli taki folder nie istnieje, zostanie utworzony. Jeśli chcesz zmienić tę ścieżkę, wskaż folder lokalny. Foldery sieciowe, w tym foldery znajdujące się na zamapowanych dyskach, nie są obsługiwane.

Ustawienie domyślne: **Włączono**.

Ochrona po stronie serwera

Ta opcja pozwala określić, czy moduł Ochrona przed wirusami i złośliwym oprogramowaniem ma chronić foldery sieciowe udostępnione przez Ciebie z poziomu połączeń zewnętrznych przychodzących z innych serwerów w sieci, które ewentualnie mogą powodować zagrożenia.

Ustawienie domyślne: **Wyłączono**.

Ustawianie zaufanych i blokowanych połączeń

Na karcie **Zaufane** można określić połączenia, w ramach których będą dozwolone zmiany danych. Trzeba zdefiniować nazwę użytkownika i adres IP.

Na karcie **Zablokowano** można określić połączenia, w ramach których nie będą dozwolone zmiany danych. Trzeba zdefiniować nazwę użytkownika i adres IP.

Ochrona własna

Ochrona własna zapobiega nieuprawnionym zmianom w procesach własnych oprogramowania, rekordach rejestru, plikach wykonywalnych i konfiguracyjnych, partycji Secure Zone oraz kopiach zapasowych przechowywanych w folderach lokalnych. Nie zalecamy wyłączania tej funkcji.

Ustawienie domyślne: **Włączono**.

Zezwalanie procesom na modyfikowanie kopii zapasowych

Opcja **Zezwól określonym procesom na modyfikowanie kopii zapasowych** działa wtedy, gdy jest włączona **Ochrona własna**.

Dotyczy ona plików o rozszerzeniach .tibx, .tib, .tia, które znajdują się w folderach lokalnych.

Ta opcja pozwala określać procesy, które mogą modyfikować pliki kopii zapasowej nawet wtedy, gdy pliki te są chronione przez funkcję ochrony własnej. Może to się przydać na przykład w przypadku zamiaru usunięcia plików kopii zapasowej lub przeniesienia ich do innej lokalizacji za pomocą skryptu.

Gdy ta opcja jest wyłączona, pliki kopii zapasowej mogą być modyfikowane wyłącznie przez proces zatwierdzony przez dostawcę oprogramowania do tworzenia kopii zapasowych. Pozwala to oprogramowaniu na stosowanie reguł przechowywania i usuwanie kopii zapasowych na żądanie użytkownika przesłane za pośrednictwem interfejsu internetowego. Inne procesy – niezależnie od tego, czy zostaną uznane za podejrzane – nie mogą modyfikować kopii zapasowych.

Gdy ta opcja jest włączona, można zezwolić innym procesom na modyfikowanie kopii zapasowych. Podaj pełną ścieżkę do wykonywalnego procesu, zaczynając od litery dysku.

Ustawienie domyślne: **Wyłączono**.

Wykrywanie procesów cryptominingu

Ta opcja pozwala określić, czy moduł Ochrona przed wirusami i złośliwym oprogramowaniem ma wykrywać ewentualne złośliwe oprogramowanie do cryptominingu.

Złośliwe oprogramowanie do cryptominingu obniża wydajność pożytecznych aplikacji i podwyższa rachunki za energię elektryczną, a generowane przez nie nadmierne obciążenie może powodować awarie systemu, a nawet uszkodzić sprzęt. Aby zapobiec uruchomieniu złośliwego oprogramowania do cryptominingu, warto je dodać do listy **Szkodliwe procesy**.

Ustawienie domyślne: **Włączono**.

Ustawienia wykrywania procesów cryptominingu

Wybierz działanie wykonywane przez oprogramowanie po wykryciu aktywności związanej z cryptominingiem, a następnie kliknij **Gotowe**. Można wybrać jedną z następujących opcji:

- **Tylko powiadom**
  Oprogramowanie wygeneruje alert dotyczący procesu podejrzewanego o działania związane z cryptominingiem.
- **Zatrzymaj proces**
  Oprogramowanie wygeneruje alert dotyczący procesu podejrzewanego o działania związane z cryptominingiem i zatrzyma ten proces.

Ustawienie domyślne: **Zatrzymaj proces**.

Kwarantanna

Kwarantanna to folder służący do izolowania podejrzanych (prawdopodobnie zainfekowanych) lub potencjalnie niebezpiecznych plików.

Usuń pliki z kwarantanny po — umożliwia określenie liczby dni, po których upłynięciu pliki poddane kwarantannie zostaną usunięte.

Ustawienie domyślne: **30 dni**.

Wykrywanie zachowań

Acronis Cyber Protect chroni system, stosując mechanizmy heurystyki behawioralnej w celu rozpoznawania złośliwych procesów: porównuje łańcuch działań wykonywanych przez proces z łańcuchami działań zapisanymi w bazie danych wzorców złośliwego zachowania. Tak właśnie jest wykrywane nowe złośliwe oprogramowanie — na podstawie jego typowego zachowania.

Ustawienie domyślne: **Włączono**.

Ustawienia wykrywania zachowań

W obszarze **Działanie po wykryciu** wybierz działanie wykonywane przez oprogramowanie po wykryciu działania złośliwego oprogramowania, a następnie kliknij **Gotowe**.

Można wybrać jedną z następujących opcji:

- **Tylko powiadom**
  Oprogramowanie wygeneruje alert dotyczący procesu podejrzewanego o działania związane ze złośliwym oprogramowaniem.
- **Zatrzymaj proces**
  Oprogramowanie wygeneruje alert i zatrzyma proces podejrzewany o działania związane ze złośliwym oprogramowaniem.
- **Kwarantanna**
  Oprogramowanie wygeneruje alert, zatrzyma proces i przeniesie plik wykonywalny do folderu kwarantanny.

Ustawienie domyślne: **Kwarantanna**.

Ochrona w czasie rzeczywistym

Funkcja **Ochrona w czasie rzeczywistym** stale sprawdza system komputerowy pod kątem wirusów i innych zagrożeń, gdy system jest włączony.

Ustawienie domyślne: **Włączono**.

Konfigurowanie działania po wykryciu na potrzeby ochrony w czasie rzeczywistym

W obszarze **Działanie po wykryciu** wybierz działanie wykonywane przez oprogramowanie po wykryciu wirusa lub innego złośliwego zagrożenia, a następnie kliknij **Gotowe**.

Można wybrać jedną z następujących opcji:

- **Zablokuj i powiadom**
  Oprogramowanie blokuje proces i generuje alert dotyczący procesu podejrzewanego o działania związane ze złośliwym oprogramowaniem.
- **Kwarantanna**
  Oprogramowanie generuje alert, zatrzymuje proces i przenosi plik wykonywalny do folderu kwarantanny.

Ustawienie domyślne: **Kwarantanna**.

Konfigurowanie trybu skanowania na potrzeby ochrony w czasie rzeczywistym

W obszarze **Tryb skanowania** wybierz działanie wykonywane przez oprogramowanie po wykryciu wirusa lub innego złośliwego zagrożenia, a następnie kliknij **Gotowe**.

Można wybrać jedną z następujących opcji:

- **Inteligentne przy dostępie** — skanowanie uruchamiane przy dostępie monitoruje wszystkie działania w systemie i automatycznie skanuje pliki, gdy są one otwierane w celu odczytania lub zapisania oraz gdy jest uruchamiany program.
- **Skanowanie przy wykonywaniu** — automatycznie są skanowane tylko pliki wykonywalne w chwili ich uruchamiania w celu sprawdzenia, czy nie są one zainfekowane i nie spowodują żadnych uszkodzeń komputera ani danych.

Ustawienie domyślne: **Inteligentne przy dostępie**.

Zaplanuj skanowanie

Włączając ustawienie **Zaplanuj skanowanie**, można zdefiniować harmonogram, według którego komputer będzie sprawdzany pod kątem złośliwego oprogramowania.

Działanie po wykryciu:

- **Kwarantanna**
  Oprogramowanie generuje alert i przenosi plik wykonywalny do folderu kwarantanny.
- **Tylko powiadom**
  Oprogramowanie generuje alert dotyczący procesu podejrzewanego o działania związane ze złośliwym oprogramowaniem.

Ustawienie domyślne: **Kwarantanna**.

Typ skanowania:

- **Pełne**
  Pełne skanowanie trwa znacznie dłużej niż szybkie skanowanie, ponieważ w tym przypadku jest sprawdzany każdy plik.
- **Szybkie**
  W ramach szybkiego skanowania są sprawdzane tylko typowe obszary na komputerze, w których zwykle znajduje się złośliwe oprogramowanie.
- **Niestandardowe**
  Skanowanie niestandardowe umożliwia sprawdzenie plików/folderów wybranych przez administratora do planu ochrony.

W jednym planie ochrony można uwzględnić wszystkie trzy tryby skanowania: **Szybkie**, **Pełne** i **Niestandardowe**.

Ustawienia domyślne:

- Zaplanowano skanowanie **Szybkie** i **Pełne**.
- Skanowanie **Niestandardowe** jest domyślnie wyłączone.

Zaplanuj wykonanie zadania przy użyciu następujących zdarzeń:

- **Zaplanuj według czasu** — zadanie zostanie uruchomione w określonym czasie.
- **Gdy użytkownik zaloguje się w systemie** — domyślnie zalogowanie się dowolnego użytkownika spowoduje uruchomienie zadania. Można zmodyfikować to ustawienie tak, aby zadanie było wyzwalane tylko przez określone konto użytkownika.
- **Gdy użytkownik wyloguje się z systemu** — domyślnie wylogowanie się dowolnego użytkownika spowoduje uruchomienie zadania. Można zmodyfikować to ustawienie tak, aby zadanie było wyzwalane tylko przez określone konto użytkownika.

Uwaga
Zadanie nie zostanie uruchomione przy zamykaniu systemu. Zamknięcie systemu i wylogowanie to różne zdarzenia w konfiguracji harmonogramu.

- **Podczas uruchamiania systemu** — zadanie zostanie uruchomione podczas uruchamiania systemu operacyjnego.
- **Podczas zamknięcia systemu** — zadanie zostanie uruchomione podczas zamykania systemu operacyjnego.

Ustawienie domyślne: **Zaplanuj według czasu**.

Typ harmonogramu:

- **Co miesiąc** — należy wybrać miesiące i tygodnie lub dni miesiąca, w których zadanie będzie uruchamiane.
- **Codziennie** — należy wybrać dni tygodnia, w których zadanie będzie uruchamiane.
- **Co godzinę** — należy wybrać dni tygodnia, liczbę powtórzeń oraz przedział czasu, w których zadanie będzie uruchamiane.

Ustawienie domyślne: **Codziennie**.

Rozpocznij o — należy wybrać dokładną godzinę, o której zadanie zostanie uruchomione.

Uruchom w podanym okresie — należy ustawić zakres czasu, w którym będzie obowiązywać skonfigurowany harmonogram.

Warunki uruchomienia — należy określić wszystkie warunki, które muszą być jednocześnie spełnione, aby zostało uruchomione zadanie.

Warunki uruchomienia skanowania pod kątem złośliwego oprogramowania są podobne do warunków uruchomienia modułu Kopia zapasowa, które opisano w "Warunki rozpoczęcia" (s. 248). Można zdefiniować następujące dodatkowe warunki uruchomienia:

- **Rozłóż rozpoczęcie zadania w przedziale czasu** — ta opcja umożliwia zdefiniowanie ram czasowych zadań, aby uniknąć wąskich gardeł na łączach sieciowych. Możesz określić opóźnienie w godzinach lub minutach. Jeśli na przykład domyślną godziną rozpoczęcia jest 10:00, a opóźnienie wynosi 60 minut, to zadanie rozpocznie się między godziną 10:00 a 11:00.
- **Jeśli komputer jest wyłączony, uruchom pominięte zadania przy jego uruchamianiu**

- **Zablokuj włączanie trybu uśpienia lub hibernacji podczas wykonywania zadania** — ta opcja działa tylko w przypadku komputerów z systemem Windows.
- **Nawet jeśli warunki uruchomienia nie są spełnione, wykonaj zadanie po** — określ czas, po którym zadanie zostanie uruchomione, bez względu na spełnienie innych warunków rozpoczęcia.

Skanuj tylko nowe i zmienione pliki — zostaną przeskanowane tylko nowo utworzone i zmodyfikowane pliki.

Ustawienie domyślne: **Włączono**.

Planując **Pełne skanowanie**, masz dostęp do dwóch dodatkowych opcji:

- **Skanuj pliki archiwum**
  Ustawienie domyślne: **Włączono**.
  - **Maksymalna głębokość rekursji**
    Liczba poziomów osadzonych archiwów, które można przeskanować. Na przykład dokument MIME > archiwum ZIP > archiwum pakietu Office > zawartość dokumentu.
    Ustawienie domyślne: **16**.
  - **Maksymalny rozmiar**
    Maksymalny rozmiar pliku archiwum do przeskanowania.
    Ustawienie domyślne: **Bez ograniczeń**.
- **Skanuj dyski wymienne**
  Ustawienie domyślne: **Wyłączono**.
  - **Zamapowane (zdalne) dyski sieciowe**
  - **Urządzenia pamięci USB** (takie jak dyski flash i zewnętrzne dyski twarde)
  - **Dyski CD/DVD**

Wykluczenia

W celu minimalizacji zasobów zużywanych przez analizę heurystyczną i wyeliminowania tak zwanych wyników fałszywie dodatnich, gdy zaufany program jest uważany za oprogramowanie wymuszające okup, możesz zdefiniować następujące ustawienia:

Na karcie **Zaufane** można wskazać:

- Procesy, które nigdy nie będą uznawane za złośliwe oprogramowanie. Procesy podpisane przez firmę Microsoft są zawsze zaufane.
- Foldery, w których przypadku zmiany w plikach nie będą monitorowane.
- Pliki i foldery, które nie będą uwzględniane w ramach zaplanowanego skanowania.

Na karcie **Zablokowano** można wskazać:

- Procesy, które zawsze będą blokowane. Dopóki na komputerze jest włączona funkcja Active Protection, procesy te nie będą mogły się rozpocząć.
- Foldery, w których będą blokowane wszystkie procesy.

Podaj pełną ścieżkę do wykonywalnego procesu, zaczynając od litery dysku. Na przykład: `C:\Windows\Temp\er76s7sdkh.exe`.

W celu określenia folderów można używać symboli wieloznacznych * i ?. Gwiazdka (*) zastępuje zero lub więcej znaków. Znak zapytania (?) zastępuje dokładnie jeden znak. Nie można używać zmiennych środowiskowych, takich jak `%AppData%`.

Ustawienie domyślne: Domyślnie nie ma zdefiniowanych żadnych wyjątków.

Filtrowanie adresów URL

Szczegółowy opis można znaleźć w sekcji Filtrowanie adresów URL.

Active Protection

W wersjach Cyber Backup programu Acronis Cyber Protect: Active Protection jest osobnym modułem w planie ochrony. Moduł ten ma następujące ustawienia:

- Działanie po wykryciu
- Ochrona własna
- Ochrona folderów sieciowych
- Ochrona po stronie serwera
- Wykrywanie procesów cryptominingu
- Wykluczenia

W wersjach Protect programu Acronis Cyber Protect: Active Protection wchodzi w skład modułu Ochrona przed wirusami i złośliwym oprogramowaniem.

Usługa Active Protection jest dostępna dla komputerów z następującymi systemami operacyjnymi:

- Systemy operacyjne na komputerach stacjonarnych: Windows 7 Service Pack 1 lub nowszy
  W przypadku komputerów z systemem Windows 7 dopilnuj, aby była zainstalowana aktualizacja systemu Windows 7 (KB2533623).
- Systemy operacyjne na serwerach: Windows Server 2008 R2 lub nowszy.

Na komputerze musi być zainstalowany agent dla systemu Windows.

Więcej informacji o module Active Protection i jego ustawieniach można znaleźć w "Ustawienia modułu Ochrona przed wirusami i złośliwym oprogramowaniem" (s. 530).

Program antywirusowy Windows Defender

Program antywirusowy Windows Defender to wbudowany komponent ochrony antywirusowej udostępniany wraz z systemem Microsoft Windows, począwszy od wersji Windows 8.

Moduł Program antywirusowy Windows Defender pozwala skonfigurować zasady zabezpieczeń programu antywirusowego Windows Defender i monitorować ich status za pomocą konsoli internetowej Cyber Protect.

Moduł ten ma zastosowanie do komputerów, na których jest zainstalowany program antywirusowy Windows Defender.

Zaplanuj skanowanie

Określ harmonogram planowanych operacji skanowania.

Tryb skanowania:

- **Pełne** — pełne sprawdzenie wszystkich plików i folderów oprócz elementów skanowanych podczas szybkiego skanowania. Takie skanowanie wymaga więcej zasobów komputera niż szybkie skanowanie.
- **Szybkie** — szybkie sprawdzenie procesów w pamięci oraz folderów, w których zwykle wykrywa się złośliwe oprogramowanie. Takie skanowanie wymaga mniej zasobów komputera niż pełne skanowanie.

Należy określić godzinę i dzień tygodnia, w którym będzie wykonywane.

Codziennie szybkie skanowanie — należy określić godzinę codziennego szybkiego skanowania.

W zależności od potrzeb można włączyć jedną z opcji:

Rozpocznij zaplanowane skanowanie, gdy komputer jest włączony, ale nie jest używany

Przed zaplanowanym skanowaniem sprawdź dostępność najnowszych definicji wirusów i oprogramowania szpiegowskiego

Ogranicz obciążenie procesora podczas skanowania do

Więcej informacji na temat ustawień harmonogramu programu antywirusowego Windows Defender można znaleźć pod adresem https://docs.microsoft.com/en-us/sccm/protect/deploy-use/endpoint-antimalware-policies#scheduled-scans-settings.

Czynności domyślne

Zdefiniuj domyślne działania, które mają być wykonywane w przypadku wykrytych zagrożeń o różnych poziomach ważności:

- **Wyczyść** — wykryte złośliwe oprogramowanie zostaje wyczyszczone z komputera.
- **Kwarantanna** — wykryte złośliwe oprogramowanie zostaje umieszczone w folderze kwarantanny, ale nie usunięte.
- **Usuń** — wykryte złośliwe oprogramowanie zostaje usunięte z komputera.
- **Pozwól** — wykryte złośliwe oprogramowanie nie zostaje usunięte ani poddane kwarantannie.
- **Określone przez użytkownika** — użytkownik otrzymuje monit o określenie, co należy zrobić z wykrytym złośliwym oprogramowaniem.

- **Brak czynności** — żadne czynności nie są podejmowane.
- **Blokuj** — wykryte złośliwe oprogramowanie zostaje zablokowane.

Więcej informacji na temat ustawień domyślnych czynności programu antywirusowego Windows Defender można znaleźć pod adresem https://docs.microsoft.com/en-us/sccm/protect/deploy-use/endpoint-antimalware-policies#default-actions-settings.

Ochrona w czasie rzeczywistym

Włącz opcję **Ochrona w czasie rzeczywistym**, aby aktywować wykrywanie złośliwego oprogramowania oraz blokowanie jego instalacji lub uruchamiania na komputerach.

Skanuj wszystkie pobierane pliki — w przypadku zaznaczenia tej opcji będą skanowane wszystkie pobierane pliki i załączniki.

Włącz monitorowanie zachowań — w przypadku zaznaczenia tej opcji zostanie włączone monitorowanie zachowań.

Skanuj pliki sieciowe — w przypadku zaznaczenia tej opcji będą skanowane pliki sieciowe.

Zezwól na pełne skanowanie zamapowanych dysków sieciowych — w przypadku zaznaczenia tej opcji będą w pełni skanowane dyski sieciowe.

Zezwól na skanowanie poczty e-mail — w przypadku zaznaczenia tej opcji będą skanowane pliki skrzynki pocztowej, w zależności od ich formatu, w celu analizowania treści i załączników wiadomości e-mail.

Więcej informacji na temat ustawień ochrony w czasie rzeczywistym programu antywirusowego Windows Defender można znaleźć pod adresem https://docs.microsoft.com/en-us/sccm/protect/deploy-use/endpoint-antimalware-policies#real-time-protection-settings.

Zaawansowany

Określ zaawansowane ustawienia skanowania:

- **Skanuj pliki archiwum** — powoduje przeskanowanie również plików archiwów, takich jak .zip czy .rar.
- **Skanuj dyski wymienne** — powoduje przeskanowanie dysków wymiennych w ramach pełnego skanowania.
- **Utwórz punkt przywracania systemu** — czasem ważny plik lub wpis w rejestrze może zostać usunięty jako „fałszywy alarm”, a wówczas można go odzyskać z punktu przywracania.
- **Usuń pliki z kwarantanny po** — umożliwia określenie, po jakim czasie pliki poddane kwarantannie zostaną usunięte.
- **Automatycznie wysyłaj próbki plików, gdy jest wymagana dodatkowa analiza:**
  - **Zawsze monituj** — przed wysłaniem pliku pojawi się monit o potwierdzenie.

    - **Automatycznie wysyłaj bezpieczne próbki** — większość próbek będzie wysyłanych automatycznie, z wyjątkiem plików, które mogą zawierać dane osobowe. Takie pliki będą wymagały dodatkowego potwierdzenia.
    - **Automatycznie wysyłaj wszystkie próbki** — wszystkie próbki będą wysyłane automatycznie.
- **Wyłącz interfejs programu antywirusowego Windows Defender** — w przypadku zaznaczenia tej opcji interfejs użytkownika programu antywirusowego Windows Defender nie będzie dostępny dla użytkownika. Zasadami zabezpieczeń programu antywirusowego Windows Defender można zarządzać w konsoli internetowej Cyber Protect.
- **MAPS (Microsoft Active Protection Service)** — społeczność online, która pomaga wybrać sposób reagowania na potencjalne zagrożenia.
    - **Nie chcę dołączać do MAPS** — do firmy Microsoft nie będą wysyłane żadne informacje o wykrytym oprogramowaniu.
    - **Podstawowe członkostwo** — do firmy Microsoft będą wysyłane podstawowe informacje o wykrytym oprogramowaniu.
    - **Zaawansowane członkostwo** — do firmy Microsoft będą wysyłane szczegółowe informacje o wykrytym oprogramowaniu.

    Więcej informacji można znaleźć pod adresem https://www.microsoft.com/security/blog/2015/01/14/maps-in-the-cloud-how-can-it-help-your-enterprise.

Więcej informacji na temat zaawansowanych ustawień programu antywirusowego Windows Defender można znaleźć pod adresem https://docs.microsoft.com/en-us/sccm/protect/deploy-use/endpoint-antimalware-policies#advanced-settings.

Wykluczenia

Ze skanowania można wykluczyć następujące pliki i foldery:

- **Procesy** — ze skanowania zostanie wykluczony każdy plik, z którego odczytuje lub w którym zapisuje zdefiniowany proces. Należy zdefiniować pełną ścieżkę do pliku wykonywalnego procesu.
- **Pliki i foldery** — ze skanowania zostaną wykluczone wskazane pliki i foldery. Należy zdefiniować pełną ścieżkę do folderu lub pliku lub zdefiniować rozszerzenie pliku.

Więcej informacji na temat ustawień wykluczeń programu antywirusowego Windows Defender można znaleźć pod adresem https://docs.microsoft.com/en-us/sccm/protect/deploy-use/endpoint-antimalware-policies#exclusion-settings.

Microsoft Security Essentials

Microsoft Security Essentials to wbudowany komponent ochrony antywirusowej udostępniany wraz z systemem Microsoft Windows, począwszy od wersji Windows 8.

Moduł Microsoft Security Essentials umożliwia skonfigurowanie zasad zabezpieczeń programu Microsoft Security Essentials i monitorowanie ich statusu za pomocą konsoli internetowej Cyber Protect.

Moduł ten ma zastosowanie do komputerów, na których jest zainstalowany program Microsoft Security Essentials.

Ustawienia modułu Microsoft Security Essentials są niemal takie same jak w przypadku programu antywirusowego Microsoft Windows Defender, tyle że brak w nich ustawień ochrony w czasie rzeczywistym i brak możliwości zdefiniowania wykluczeń za pomocą konsoli internetowej Cyber Protect.

Filtrowanie adresów URL

Złośliwe oprogramowanie jest często rozprowadzane przez złośliwe lub zainfekowane witryny internetowe i wykorzystuje metodę infekcji „drive-by download", czyli niepożądane pobieranie plików. Filtrowanie adresów URL umożliwia chronienie komputerów przed takimi zagrożeniami pochodzącymi z Internetu jak złośliwe oprogramowanie czy phishing. Można blokować dostęp użytkowników do witryn internetowych, które mogą mieć złośliwą zawartość.

Filtrowanie adresów URL pozwala również na kontrolowanie użytkowania stron internetowych w celu zapewnienia zgodności z zewnętrznymi przepisami lub wewnętrznymi zasadami firmy. Można skonfigurować różne zasady dostępu dla ponad 40 kategorii witryn internetowych.

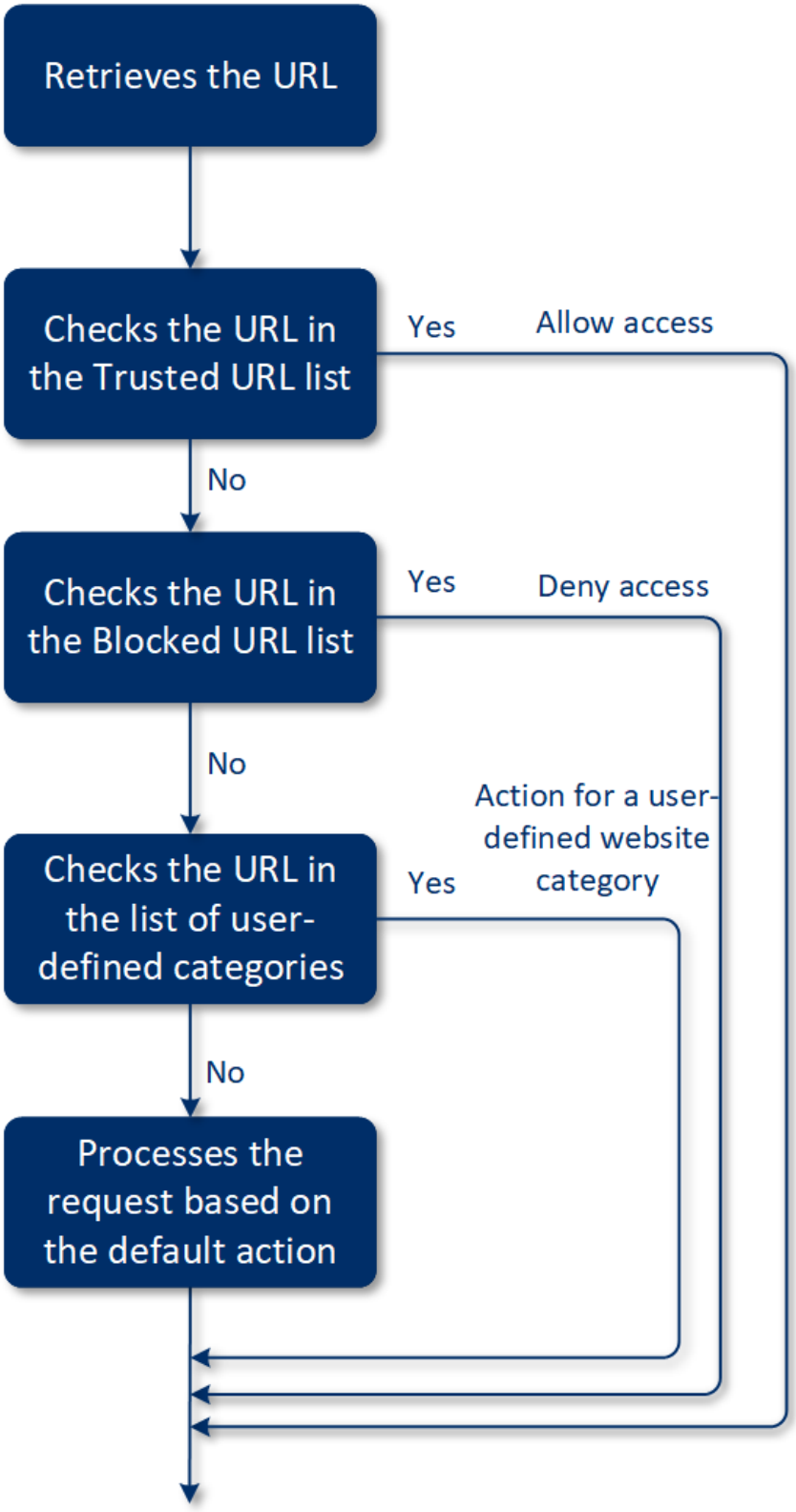
Teraz połączenia HTTP i HTTPS z komputerów z systemem Windows są sprawdzane przez agenta ochrony.

Funkcja Filtrowanie adresów URL wymaga do działania połączenia z Internetem.

Uwaga
Jeśli korzystasz z funkcji Filtrowanie adresów URL i rozwiązań antywirusowych innych firm, które również stosują filtrowanie adresów URL, mogą wystąpić konflikty. Statusy innych zainstalowanych rozwiązań antywirusowych można ustalić za pośrednictwem Centrum zabezpieczeń systemu Windows.
Jeśli wystąpi problem z kompatybilnością lub wydajnością, odinstaluj rozwiązanie innej firmy lub wyłącz moduł Filtrowanie adresów URL w planach ochrony.

Sposób działania

Użytkownik klika łącze lub wpisuje adres URL w pasku adresu przeglądarki. Kolektor rejestruje adres URL i przesyła go do agenta ochrony. Agent ochrony analizuje adres URL, sprawdza bazę danych, a następnie zwraca werdykt do Kolektora. Jeśli adres URL jest wzbroniony, Kolektor blokuje dostęp do niego i powiadamia użytkownika, że nie może zobaczyć danej zawartości.



Aby skonfigurować filtrowanie adresów URL

1. Utwórz plan ochrony z włączonym modułem Filtrowanie adresów URL.
2. Skonfiguruj ustawienia filtrowania adresów URL (patrz poniżej).

3. Przypisz plan ochrony do wybranych komputerów.

Aby sprawdzić zablokowane adresy URL, przejdź do sekcji **Panel** > **Alerty**.

Ustawienia modułu Filtrowanie adresów URL

W przypadku modułu Filtrowanie adresów URL można skonfigurować następujące ustawienia.

Dostęp do złośliwych witryn internetowych

Określ działanie, które ma zostać wykonane, gdy użytkownik spróbuje wyświetlić złośliwą witrynę internetową:

- **Zablokuj** — dostęp do złośliwej witryny internetowej zostanie zablokowany i zostanie wygenerowany alert.
- **Zawsze pytaj użytkownika** — pojawi się monit, by użytkownik wybrał, czy chce przejść do danej witryny, czy wrócić.

Kategorie do filtrowania

Dostępne są 44 kategorie witryn internetowych, których można użyć do konfigurowania zasad dostępu. Domyślnie jest dozwolony dostęp do witryn internetowych ze wszystkich kategorii.

	Kategoria witryny internetowej	Opis
1	**Reklamy**	Ta kategoria obejmuje domeny, których głównym celem jest wyświetlanie reklam.
2	**Tablice ogłoszeń**	Ta kategoria obejmuje fora, tablice dyskusyjne oraz strony internetowe typu „pytanie — odpowiedź”. Ta kategoria nie obejmuje części firmowych witryn internetowych, w których klienci zadają pytania.
3	**Osobiste witryny internetowe**	Ta kategoria obejmuje zarówno osobiste witryny internetowe, jak i wszelkiego rodzaju blogi: indywidualne, grupowe, a nawet firmowe. Blog to dziennik publikowany w sieci World Wide Web. Składa się on z wpisów („postów”) wyświetlanych zwykle w odwrotnej kolejności chronologicznej, tak że jako pierwszy pojawia się najnowszy post.
4	**Firmowe witryny internetowe**	To jest szeroka kategoria, obejmująca firmowe witryny internetowe, które zwykle nie należą do żadnej innej kategorii.
5	**Oprogramowanie komputerowe**	Ta kategoria obejmuje witryny internetowe udostępniające oprogramowanie komputerowe, zazwyczaj typu open source, freeware lub shareware. Może ona również obejmować niektóre sklepy z oprogramowaniem online.
6	**Leki**	Ta kategoria obejmuje witryny internetowe związane z lekami, alkoholami i papierosami/cygarami, w których są prowadzone dyskusje na temat

		stosowania lub sprzedaży (legalnych) leków i związanych z nimi akcesoriów, alkoholu bądź wyrobów tytoniowych. Należy pamiętać, że nielegalne substancje są uwzględniane w kategorii Narkotyki.
7	**Edukacja**	Ta kategoria obejmuje witryny internetowe należące do oficjalnych instytucji edukacyjnych, również spoza domeny .edu. Uwzględniono w niej również witryny edukacyjne, np. encyklopedie.
8	**Rozrywka**	Ta kategoria obejmuje witryny internetowe, które udostępniają informacje związane z działalnością artystyczną i muzeami, a także witryny internetowe z recenzjami i ocenami różnych dzieł, takich jak filmy, muzyka czy sztuka.
9	**Udostępnianie plików**	Ta kategoria obejmuje witryny internetowe służące do udostępniania plików, do których użytkownik może przesyłać pliki, by udostępniać je innym. Obejmuje ona również witryny służące do udostępniania torrentów oraz trackery torrentów.
10	**Finanse**	Ta kategoria obejmuje witryny internetowe należące do wszelkich banków z całego świata oferujących dostęp przez Internet. Należą do niej również niektóre unie kredytowe i inne instytucje finansowe. Jednak niektóre lokalne banki mogą nie być w niej ujęte.
11	**Gry hazardowe**	Ta kategoria obejmuje hazardowe witryny internetowe. Są to witryny typu „kasyno online" lub „loteria online", które zazwyczaj wymagają płatności, zanim użytkownik będzie mógł grać na pieniądze w ruletkę, pokera, blackjacka lub podobne gry online. Niektóre z nich są legalne, co oznacza, że jest szansa na wygraną, a niektóre fałszywe, co oznacza, że nie ma szans na wygraną. Rozpoznawane są również witryny z „niezawodnymi sposobami" na zarabianie pieniędzy na hazardzie i loteriach online.
12	**Gry**	Ta kategoria obejmuje witryny internetowe udostępniające gry online, zazwyczaj oparte na apletach Adobe Flash lub JAVA. Nie ma znaczenia, czy gra jest darmowa, czy wymaga abonamentu, jednak witryny internetowe typu kasyno są wykrywane w kategorii Gry hazardowe. Oto czego ta kategoria nie obejmuje: • Oficjalne witryny internetowe firm produkujących gry wideo (pod warunkiem, że nie produkują one gier online) • Witryny internetowe będące miejscami dyskusji o grach • Witryny internetowe, z których można pobierać gry działające w trybie offline (niektóre z nich znajdują się w kategorii Nielegalne pobieranie plików). • Gry, które wymagają od użytkownika pobrania i uruchomienia pliku wykonywalnego, takie jak World of Warcraft — można temu zapobiec za pomocą różnych środków, na przykład zapory.
13	**Administracja**	Ta kategoria obejmuje witryny internetowe administracji publicznej, w tym

	publiczna	urzędów, państwowych instytucji i ambasad.
14	**Hakowanie**	Ta kategoria obejmuje witryny internetowe, które udostępniają narzędzia, artykuły i platformy dyskusyjne dla hakerów. Obejmuje ona również witryny oferujące exploity do popularnych platform, które ułatwiają hakowanie kont na Facebooku lub Gmailu.
15	**Nielegalne działania**	To jest szeroka kategoria związana z nienawiścią, przemocą i rasizmem, umożliwiająca blokowanie następujących rodzajów witryn internetowych: • Witryny należące do organizacji terrorystycznych • Witryny zawierające treści rasistowskie lub ksenofobiczne • Witryny będące miejscami dyskusji o agresywnych sportach i/lub promujące przemoc
16	**Zdrowie i fitness**	Ta kategoria obejmuje witryny internetowe instytucji opieki zdrowotnej oraz dotyczące profilaktyki i leczenia chorób, witryny udostępniające informacje lub produkty związane z odchudzaniem, żywieniem, sterydami, anabolikami czy hormonami wzrostu, a także witryny z informacjami o operacjach plastycznych.
17	**Hobby**	Ta kategoria obejmuje witryny internetowe, które oferują materiały i produkty związane z działaniami wykonywanymi na ogół w czasie wolnym od pracy, takimi jak kolekcjonerstwo, sztuka i rzemiosło czy jazda na rowerze.
18	**Hosting witryn internetowych**	Ta kategoria obejmuje bezpłatne i komercyjne usługi hostingowe, które umożliwiają prywatnym użytkownikom oraz firmom i instytucjom tworzenie i publikowanie stron internetowych.
19	**Nielegalne pobieranie plików**	Ta kategoria obejmuje witryny internetowe umożliwiające piractwo oprogramowania, takie jak: • Witryny do śledzenia peer-to-peer (BitTorrent, emule, DC++) znane z ułatwiania rozpowszechniania treści chronionych prawami autorskimi bez zgody właścicieli praw autorskich • Witryny internetowe i tablice ogłoszeń związane z warezami (spiratowanym oprogramowaniem komercyjnym) • Witryny internetowe udostępniające użytkownikom cracki, generatory kluczy i numery seryjne umożliwiające nielegalne korzystanie z oprogramowania. Niektóre z tych witryn internetowych mogą też być wykrywane jako pornografia lub alkohol/papierosy, ponieważ często w celach zarobkowych są w nich zamieszczane reklamy pornografii lub alkoholu.
20	**Komunikatory i czaty**	Ta kategoria obejmuje komunikatory internetowe i czaty, które umożliwiają rozmawianie w czasie rzeczywistym. W jej ramach będą wykrywane również witryny yahoo.com i gmail.com, ponieważ obie mają wbudowane komunikatory internetowe.

21	**Oferty pracy**	Ta kategoria obejmuje witryny internetowe z tablicami ogłoszeń o pracę albo reklamami związanymi z ofertami pracy i możliwościami rozwoju kariery, a także agregatory takich usług. Nie obejmuje ona agencji rekrutacyjnych ani stron „ofert pracy" w zwykłych firmowych witrynach internetowych.
22	**Treści dla osób dojrzałych**	Ta kategoria obejmuje treści, które zostały oznaczone przez twórcę witryny internetowej jako wymagające dojrzałej publiczności. Obejmuje ona szeroką gamę witryn internetowych: od poświęconych książce Kama Sutra i edukacji seksualnej po twardą pornografię.
23	**Narkotyki**	Ta kategoria obejmuje witryny internetowe udostępniające informacje o rekreacyjnych i nielegalnych narkotykach. Obejmuje ona również witryny dotyczące produkcji lub uprawy narkotyków.
24	**Wiadomości**	Ta kategoria obejmuje witryny internetowe z informacjami w formie tekstowej i wideo. W kategorii tej próbuje się uwzględniać wszelkie — zarówno globalne, jak i lokalne — serwisy informacyjne, jednak niektóre małe, lokalne serwisy informacyjne mogą nie być nią objęte.
25	**Randki online**	Ta kategoria obejmuje randkowe witryny internetowe — płatne i bezpłatne — w których użytkownicy mogą wyszukiwać inne osoby według wybranych kryteriów. Mogą też umieszczać własne profile, aby inni mogli je wyszukiwać. Ta kategoria obejmuje zarówno darmowe, jak i płatne witryny randkowe. Ponieważ większość popularnych portali społecznościowych może pełnić funkcję witryn randkowych, niektóre z nich, np. Facebook, również są wykrywane w tej kategorii. Warto korzystać z tej kategorii w połączeniu z kategorią Portale społecznościowe.
26	**Płatności online**	Ta kategoria obejmuje witryny internetowe obsługujące płatności online lub przelewy pieniężne. Wykrywane są w niej popularne witryny obsługujące płatności, takie jak PayPal czy Moneybookers. Ponadto w zwykłych witrynach heurystycznie wykrywane są strony z monitami o podanie danych karty kredytowej, co pozwala na wykrycie ukrytych, nieznanych lub nielegalnych sklepów internetowych.
27	**Udostępnianie zdjęć**	Ta kategoria obejmuje witryny internetowe, których głównym celem jest umożliwienie użytkownikom zamieszczania i udostępniania zdjęć.
28	**Sklepy online**	Ta kategoria obejmuje znane sklepy internetowe. Witryna internetowa jest uznawana za sklep internetowy, jeśli sprzedaje towary lub usługi online.
29	**Pornografia**	Ta kategoria obejmuje witryny internetowe zawierające treści erotyczne i pornograficzne. Obejmuje ona zarówno płatne, jak i bezpłatne witryny ze zdjęciami, opowiadaniami i filmami. Wykrywane są też treści pornograficzne w witrynach z różnorodną zawartością.
30	**Portale**	Ta kategoria obejmuje witryny internetowe, które agregują informacje z wielu źródeł oraz różnych domen i które zwykle udostępniają takie funkcje

		jak wyszukiwarki, poczta e-mail oraz informacje o wydarzeniach lub dotyczące rozrywki.
31	**Radio**	Ta kategoria obejmuje witryny internetowe, które oferują strumieniową transmisję muzyki — od internetowych stacji radiowych po witryny udostępniające treści audio na żądanie (bezpłatne lub płatne).
32	**Religia**	Ta kategoria obejmuje witryny internetowe promujące religię lub sektę. Obejmuje ona również fora dyskusyjne związane z jedną lub wieloma religiami.
33	**Wyszukiwarki**	Ta kategoria obejmuje wyszukiwarki internetowe, takie jak Google, Yahoo i Bing.
34	**Portale społecznościowe**	Ta kategoria obejmuje portale społecznościowe, np. MySpace.com, Facebook.com, Bebo.com itp. Jednak wyspecjalizowane portale społecznościowe, takie jak YouTube.com, będą wymieniane w kategorii Filmy/zdjęcia.
35	**Sport**	Ta kategoria obejmuje witryny internetowe, które oferują informacje sportowe, wiadomości i instruktaże.
36	**Samobójstwa**	Ta kategoria obejmuje witryny internetowe promujące samobójstwa i nawołujące do nich. Nie obejmuje ona klinik profilaktyki samobójstw.
37	**Tabloidy**	Ta kategoria dotyczy głównie witryn internetowych z miękką pornografią i plotkami o gwiazdach. Wiele witryn internetowych z tabloidowymi wiadomościami może mieć wymienione tu podkategorie. W tej kategorii również wykrywanie jest oparte na heurystyce.
38	**Marnotrawstwo czasu**	Ta kategoria obejmuje witryny internetowe, w których użytkownicy spędzają mnóstwo czasu. Mogą się niej znaleźć witryny z innych kategorii, na przykład portale społecznościowe lub witryny rozrywkowe.
39	**Podróże**	Ta kategoria obejmuje witryny internetowe, w których są prezentowane oferty wyjazdów turystycznych i sprzętu turystycznego, a także opinie i oceny dotyczące celów podróży.
40	**Wideo**	Ta kategoria obejmuje witryny internetowe, w których są dostępne filmy lub zdjęcia przesyłane przez użytkowników bądź dostarczane przez różnych dostawców treści. Dotyczy to na przykład witryn YouTube, Metacafe i Google Video, a także witryn ze zdjęciami, takich jak Picasa czy Flickr. Będą wykrywane również filmy wideo osadzone w innych witrynach lub blogach.
41	**Brutalne kreskówki**	Ta kategoria obejmuje witryny internetowe omawiające, udostępniające i oferujące brutalne kreskówki lub mangi, które mogą być nieodpowiednie dla osób nieletnich ze względu na przemoc, wulgaryzmy lub treści seksualne. Kategoria ta nie obejmuje witryn udostępniających kreskówki z głównego

		nurtu, takich jak „Tom i Jerry”.
42	**Broń**	Ta kategoria obejmuje witryny internetowe dotyczące sprzedaży lub wymiany, produkcji bądź użytkowania broni. Uwzględniane są tu również witryny z wyposażeniem myśliwskim oraz dotyczące korzystania z wiatrówek i pistoletów na śrut BB, a także broni używanej w walce wręcz.
43	**E-mail**	Ta kategoria obejmuje witryny internetowe, które udostępniają pocztę e-mail jako aplikację internetową.
44	**Serwer proxy WWW**	Ta kategoria obejmuje witryny internetowe udostępniające usługę serwera proxy WWW. Chodzi tu o witryny typu „przeglądarka w przeglądarce”: gdy użytkownik chcesz otworzyć stronę internetową, wpisuje jej adres URL w formularzu i klika „Prześlij” („Submit”). Witryna serwera proxy WWW pobiera daną stronę i wyświetla ją w przeglądarce użytkownika. Powody do wykrywania tego typu ruchu (i ewentualnej konieczności jego blokowania): • Anonimowe przeglądanie. Ponieważ żądania wysyłane do docelowego serwera WWW przychodzą z serwera proxy, widoczny jest tylko jego adres IP, więc jeśli administratorzy serwera spróbują wyśledzić trasę użytkownika, trop urwie się na serwerze proxy, który nie musi mieć dzienników niezbędnych do zlokalizowania inicjującego sesję użytkownika. • Spoofing lokalizacji. Adresy IP użytkowników często są używane do profilowania usługi według lokalizacji źródłowej (niektóre krajowe strony administracji publicznej mogą być dostępne tylko z lokalnych adresów IP), więc skorzystanie z takiej usługi może użytkownikowi pomóc w sfałszowaniu swojej rzeczywistej lokalizacji. • Dostęp do wzbronionych treści. Jeśli zostanie użyty prosty filtr adresów URL, będzie on wykrywał tylko adresy serwera proxy WWW, a nie adresy rzeczywistych serwerów odwiedzanych przez użytkownika. • Uniknięcie monitorowania przez pracodawcę. W firmie może obowiązywać zasada monitorowania użytkowania Internetu przez pracowników. Uzyskując dostęp do stron za pośrednictwem serwera proxy WWW, użytkownik może sprawić, że monitorowania nie zapewni firmie rzetelnych informacji. Ponieważ zestaw SDK analizuje stronę HTML (jeśli będzie dostępna), a nie tylko adres URL, w przypadku niektórych kategorii zestaw SDK nadal będzie w stanie rozpoznać wyświetlane treści. Jednak w przypadku innych powodów problemów nie da się uniknąć tylko przez zastosowanie zestawu SDK.

W przypadku zaznaczenia pola wyboru **Pokaż wszystkie powiadomienia o zablokowanych adresach URL według kategorii** na pasku zadań będą wyświetlane wszelkie powiadomienia o zablokowanych adresach URL według kategorii. Jeśli witryna internetowa obejmuje kilka poddomen,

powiadomienia będą generowane również w ich przypadku, w związku z czym liczba powiadomień może być dość duża.

Wykluczenia

Adresy URL, które są znane jako bezpieczne, można dodać do listy zaufanych adresów URL. Adresy URL, które stanowią zagrożenie, można dodać do listy blokowanych adresów URL.

Aby dodać adres URL do listy

1. W module Filtrowanie adresów URL planu ochrony kliknij **Wykluczenia**.
2. Wybierz odpowiednią listę: **Zaufane** lub **Zablokowano**.
3. Kliknij **Dodaj**.
4. Podaj adres URL lub adres IP, a następnie kliknij znacznik wyboru.

Przykład wykluczeń adresów URL:

- Jeśli dodasz xyz.com jako adres zaufany/niezaufany, wszystkie adresy w domenie xyz.com będą traktowane odpowiednio jako zaufane lub niezaufane.
- Jeśli chcesz dodać określoną poddomenę, możesz dodać **mail.xyz.com** jako zaufaną/niezaufaną, a to nie sprawi, że wszystkie adresy **xyz.com** będą zaufane lub niezaufane.
- Jeśli chcesz dodać adres IPv4 jako zaufany/niezaufany, musisz użyć następującego prawidłowego formatu: **20.53.203.50**.
- Jeśli chcesz dodać kilka wykluczeń adresów URL naraz, pamiętaj, aby dodać każdy wpis w osobnym wierszu:

  acronis.com

  mail.xyz.com

  20.53.203.50

Kwarantanna

Kwarantanna to specjalny, odizolowany folder na dysku twardym komputera, w którym są umieszczane podejrzane pliki wykryte przez moduł Ochrona przed wirusami i złośliwym oprogramowaniem, aby zapobiec dalszemu rozprzestrzenianiu się zagrożeń.

Kwarantanna pozwala na przeglądanie podejrzanych oraz potencjalnie niebezpiecznych plików ze wszystkich komputerów i decydowanie o ich usunięciu lub przywróceniu. Pliki poddane kwarantannie są automatycznie usuwane w przypadku usunięcia komputera z systemu.

Jak pliki trafiają do folderu kwarantanny?

1. Użytkownik konfiguruje plan ochrony i definiuje domyślne działanie dotyczące zainfekowanych plików — umieszczenie ich w kwarantannie.

2. Podczas skanowania zaplanowanego lub wykonywanego przy dostępie system wykrywa złośliwe pliki i umieszcza je w bezpiecznym folderze, czyli w kwarantannie.
3. System aktualizuje listę kwarantanny na poszczególnych komputerach.
4. Pliki są automatycznie czyszczone z folderu kwarantanny po upływie czasu określonego za pomocą ustawienia **Usuń pliki z kwarantanny po** w planie ochrony.

Zarządzanie plikami poddanymi kwarantannie

Aby zarządzać plikami poddanymi kwarantannie, przejdź do sekcji **Ochrona antywirusowa** > **Kwarantanna**. Zostanie wyświetlona lista z plikami poddanymi kwarantannie ze wszystkich komputerów.

Nazwa	Opis
Plik	Nazwa pliku.
Data rozpoczęcia kwarantanny	Data i godzina umieszczenia pliku w kwarantannie.
Urządzenie	Urządzenie, na którym znaleziono zainfekowany plik.
Nazwa zagrożenia	Nazwa zagrożenia.
Plan ochrony	Plan ochrony, zgodnie z którym podejrzany plik został umieszczony w kwarantannie.

W odniesieniu do plików poddanych kwarantannie można wykonać dwa działania:

- **Usuń** — trwałe usunięcie pliku poddanego kwarantannie ze wszystkich komputerów.
- **Przywróć** — przywrócenie pliku poddanego kwarantannie do pierwotnej lokalizacji bez żadnych modyfikacji. Jeśli w pierwotnej lokalizacji jest już plik o danej nazwie, zostanie on zastąpiony przywracanym plikiem.

Lokalizacja kwarantanny na komputerach

Domyślna lokalizacja plików poddanych kwarantannie to:

Na komputerze z systemem Windows: `%ProgramData%\%product_name%\Quarantine`

Na komputerze z systemem Mac/Linux: `/usr/local/share/%product_name%/quarantine`

Firmowa biała lista

Ważne
Firmowa biała lista wymaga, aby na serwerze zarządzania była zainstalowana usługa Skanowanie.

Rozwiązanie antywirusowe może rozpoznawać dozwolone aplikacje firmowe jako podejrzane. Aby zapobiec fałszywym alarmom podczas wykrywania, dodaje się zaufane aplikacje do białej listy ręcznie, a to jest czasochłonne zajęcie.

Usługa Cyber Protect może zautomatyzować ten proces: kopie zapasowe są skanowane przez moduł Ochrona przed wirusami i złośliwym oprogramowaniem, a skanowane dane są analizowane w celu przeniesienia takich aplikacji na białą listę, co zapobiega fałszywym alarmom. Ponadto ogólnofirmowa biała lista poprawia wydajność kolejnych operacji skanowania.

Białą listę można włączać lub wyłączać. Gdy jest wyłączona, dodawane do niej pliki będą tymczasowo ukrywane.

Automatyczne dodawanie pozycji do białej listy

1. Uruchom skanowanie kopii zapasowych w chmurze na co najmniej dwóch komputerach. Można to zrobić za pomocą programu "Plan skanowania kopii zapasowych" (s. 363).
2. Następnie w ustawieniach białej listy włącz przełącznik **Automatyczne generowanie białej listy**.

Ręczne dodawanie pozycji do białej listy

Nawet jeśli przełącznik **Automatyczne generowanie białej listy** jest wyłączony, można ręcznie dodać pliki do białej listy.

1. W konsoli internetowej Cyber Protect przejdź do sekcji **Ochrona przed złośliwym oprogramowaniem** > **Biała lista**.
2. Kliknij **Dodaj plik**.
3. Określ ścieżkę do pliku i kliknij **Dodaj**.

Dodawanie plików poddanych kwarantannie do białej listy

Do białej listy można dodawać pliki, które zostały poddane kwarantannie.

1. W konsoli internetowej Cyber Protect przejdź do sekcji **Ochrona przed złośliwym oprogramowaniem** > **Kwarantanna**.
2. Wybierz plik poddany kwarantannie i kliknij **Dodaj do białej listy**.

Ustawienia białej listy

W przypadku włączenia przełącznika **Automatyczne generowanie białej listy** trzeba określić jeden z następujących poziomów ochrony heurystycznej:

- **Niski**

  Firmowe aplikacje zostaną dodane do białej listy dopiero po upływie dłuższego czasu i przeprowadzeniu kontroli. Takie aplikacje są uznawane za bardziej zaufane. Strategia ta jednak

zwiększa prawdopodobieństwo fałszywych alarmów podczas wykrywania. Kryteria uznania pliku za czysty i zaufany są wysokie.

- **Domyślne**

  Firmowe aplikacje będą dodawane do białej listy zgodnie z zalecanym poziomem ochrony w celu ograniczenia ewentualnych fałszywych alarmów. Kryteria uznania pliku za czysty i zaufany są średnie.
- **Wysoki**

  Aplikacje firmowe zostaną szybciej dodane do białej listy, aby zmniejszyć liczbę potencjalnych fałszywych alarmów podczas wykrywania. Nie oznacza to jednak gwarancji niezainfekowania oprogramowania — później może ono zostać uznane za podejrzane lub za złośliwe oprogramowanie. Kryteria uznania pliku za czysty i zaufany są niskie.

Wyświetlanie szczegółowych informacji na temat pozycji z białej listy

Kliknięcie pozycji na białej liście umożliwia wyświetlenie dodatkowych informacji na jej temat i przeanalizowanie jej online.

Jeśli nie masz pewności co do dodanej pozycji, możesz ją sprawdzić w analizatorze VirusTotal. Jeśli klikniesz **Sprawdź w ramach VirusTotal**, witryna przeanalizuje podejrzane pliki i adresy URL pod kątem różnego typu złośliwego oprogramowania, korzystając ze skrótu pliku dodanej pozycji. Skrót można sprawdzić w ciągu **Skrót pliku (MD5)**.

Wartość **Komputery** reprezentuje liczbę komputerów, na których znaleziono taki skrót podczas skanowania kopii zapasowych. Wartość ta jest wypełniana tylko wtedy, gdy dana pozycja pochodzi ze skanowania kopii zapasowych lub kwarantanny. Jeśli plik został dodany do białej listy ręcznie, to pole pozostaje puste.

Skanowanie antywirusowe kopii zapasowych

Aby zapobiec przywracaniu zainfekowanych plików z kopii zapasowych, można przeskanować te kopie pod kątem złośliwego oprogramowania. Skanowanie kopii zapasowych jest obsługiwane tylko w przypadku systemów operacyjnych Windows. Ta funkcja jest dostępna tylko wtedy, gdy na serwerze Cyber Protect Management Server jest zainstalowana usługa Skanowanie.

Aby przeskanować kopie zapasowe pod kątem złośliwego oprogramowania, utwórz plan skanowania kopii zapasowych.

Uwaga
Ze względów bezpieczeństwa i wydajności zalecamy skanowanie przy użyciu specjalnie do tego wyznaczonego komputera. Komputer ten będzie mieć dostęp do wszystkich skanowanych kopii zapasowych.

Wyniki skanowania kopii zapasowych można sprawdzić w widżecie „Szczegóły skanowania kopii zapasowej" na pulpicie nawigacyjnym. Status kopii zapasowej można również sprawdzić w polu **Magazyn kopii zapasowych** > **Lokalizacje** > **<nazwa kopii zapasowej>**. Jeśli skanowanie kopii

zapasowych nie zostało wykonane, kopie zapasowe mają status **Nie przeskanowano**. Po wykonaniu skanowania kopii zapasowych ich status zostaje zmieniony na:

- **Brak złośliwego oprogramowania**
- **Wykryto złośliwe oprogramowanie**

Ograniczenia

- Skanowanie pod kątem złośliwego oprogramowania można wykonywać tylko w odniesieniu do kopii zapasowych typu **Cały komputer** lub **Dyski/woluminy**.
- Skanowane będą tylko woluminy z systemem plików NTFS oraz partycjonowaniem GPT i MBR.
- Obsługiwane lokalizacje kopii zapasowych: **Chmura**, **Folder lokalny** i **Folder sieciowy**.
- Kopie zapasowe zawierające punkty odzyskiwania w ramach ciągłej ochrony danych (CDP) można wybrać do skanowania, ale te punkty odzyskiwania zostaną wykluczone ze skanowania. Zostaną przeskanowane tylko zwykłe punkty odzyskiwania.
- W przypadku wybrania kopii zapasowej CDP w celu bezpiecznego odzyskania całego komputera zostanie on bezpiecznie odzyskany bez danych dostępnych w punkcie odzyskiwania CDP. Aby odzyskać dane CDP, uruchom odzyskiwanie przy użyciu opcji **Pliki/foldery**.

Ochrona aplikacji do współpracy i komunikacji

Obecnie powszechnie używa się aplikacji Zoom, Cisco Webex Meetings i Microsoft Teams do wideokonferencji / konferencji internetowych i komunikacji. Program Cyber Protect umożliwia ochronę tych narzędzi do współpracy.

Proces konfiguracji ochrony aplikacji Zoom, Cisco Webex Meetings i Microsoft Teams wygląda podobnie. Poniżej opisano konfigurację ochrony na przykładzie aplikacji Zoom.

Aby skonfigurować ochronę aplikacji Zoom

1. Na komputerze, na którym jest zainstalowana aplikacja do współpracy, zainstaluj agenta ochrony.
2. Zaloguj się do konsoli internetowej Cyber Protect i zastosuj plan ochrony, w którym jest włączony jeden z następujących modułów:
   - **Ochrona przed wirusami i złośliwym oprogramowaniem** (z włączonymi funkcjami **Ochrona własna** i **Active Protection**) — jeśli masz jedną z wersji Cyber Protect.
   - **Active Protection** (z włączoną funkcją **Ochrona własna**) — jeśli masz jedną z wersji Cyber Backup.
3. [Opcjonalnie] Aby aktywować automatyczną instalację aktualizacji, skonfiguruj moduł **Zarządzanie poprawkami** w planie ochrony.

W wyniku tego aplikacja Zoom zostanie objęta ochroną, w której ramach są wykonywane następujące czynności:

- Automatyczne instalowanie aktualizacji klienta Zoom
- Ochrona procesów aplikacji Zoom przed wstrzyknięciem kodu
- Blokowanie podejrzanych operacji procesów aplikacji Zoom
- Chronienie plików „hosts” przed dodawaniem domen związanych z aplikacją Zoom

Ocena luk w zabezpieczeniach i zarządzanie poprawkami

Ocena luk w zabezpieczeniach to proces identyfikacji, szacowania ilościowego i ustalania priorytetów znalezionych luk w zabezpieczeniach systemu. Moduł Ocena luk w zabezpieczeniach, korzystający z planu ochrony, umożliwia skanowanie komputerów w poszukiwaniu luk w zabezpieczeniach oraz sprawdzanie, czy systemy operacyjne oraz zainstalowane aplikacje są aktualne i prawidłowo działają.

Skanowanie w ramach oceny luk w zabezpieczeniach jest obsługiwane w przypadku komputerów z następującymi systemami operacyjnymi:

- Windows. Aby uzyskać więcej informacji, zobacz "Obsługiwane produkty firmy Microsoft i innych firm" (s. 557).
- Komputery z systemem Linux (CentOS 7/Virtuozzo/Acronis Cyber Infrastructure). Aby uzyskać więcej informacji, zobacz "Obsługiwane produkty dla systemu Linux" (s. 558).

Funkcja **Zarządzanie poprawkami** umożliwia zarządzanie poprawkami (aktualizacjami) aplikacji i systemów operacyjnych zainstalowanych na komputerach oraz dbanie o ich aktualność. Moduł Zarządzanie poprawkami pozwala na automatyczne lub ręczne zatwierdzanie instalacji aktualizacji na komputerach.

Zarządzanie poprawkami jest obsługiwane w przypadku komputerów z systemami operacyjnymi Windows. Aby uzyskać więcej informacji, zobacz "Obsługiwane produkty firmy Microsoft i innych firm" (s. 557).

Ocena luk w zabezpieczeniach

Proces oceny luk w zabezpieczeniach obejmuje następujące etapy:

1. Należy utworzyć plan ochrony z włączonym modułem Ocena luk w zabezpieczeniach, określić ustawienia oceny luk w zabezpieczeniach i przypisać plan do komputerów.
2. System — według harmonogramu lub na żądanie — wysyła do agentów ochrony polecenie uruchomienia skanowania w celu oceny luk w zabezpieczeniach.
3. Agenty otrzymują polecenie, uruchamiają mechanizmy skanowania w poszukiwaniu luk w zabezpieczeniach i podejmują działania związane ze skanowaniem.
4. Po zakończeniu skanowania agenty generują wyniki i wysyłają je do usługi monitorowania.
5. Usługa monitorowania przetwarza dane od agentów i wyświetla wyniki w widżetach oceny luk w zabezpieczeniach oraz na liście znalezionych luk.
6. Dzięki tej informacji można zdecydować, które luki w zabezpieczeniach muszą zostać usunięte.

Wyniki skanowania w celu oceny luk w zabezpieczeniach można monitorować w widżetach **Pulpit nawigacyjny** > **Przegląd** > **Luki w zabezpieczeniach / Występujące luki w zabezpieczeniach**.

Obsługiwane produkty firmy Microsoft i innych firm

Ocena luk w zabezpieczeniach jest obsługiwana w przypadku następujących produktów firmy Microsoft i innych firm dla systemów operacyjnych Windows.

Obsługiwane produkty firmy Microsoft

Systemy operacyjne na komputerach stacjonarnych:

- Windows 7 (Enterprise, Professional, Ultimate)
- Windows 8
- Windows 8.1
- Windows 10

Systemy operacyjne na serwerach:

- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2

Microsoft Office i związane z nim komponenty

- Microsoft Office 2019 (x64, x86)
- Microsoft Office 2016 (x64, x86)
- Microsoft Office 2013 (x64, x86)
- Microsoft Office 2010 (x64, x86)

Komponenty systemu Windows:

- Internet Explorer
- Microsoft Edge
- Windows Media Player
- .NET Framework
- Visual Studio i aplikacje
- Komponenty systemu operacyjnego:

Aplikacje serwerowe

- Microsoft SQL Server 2008 R2
- Microsoft SQL Server 2012

- Microsoft SQL Server 2014
- Microsoft SQL Server 2016
- Microsoft SQL Server 2017
- Microsoft SQL Server 2019
- Microsoft Exchange Server 2013
- Microsoft Sharepoint Server 2016
- Microsoft Sharepoint Server 2016

Obsługiwane produkty innych firm przeznaczone do systemu operacyjnego Windows

Cyber Protect obsługuje funkcje oceny luk w zabezpieczeniach i instalowania poprawek w przypadku wielu aplikacji innych firm, w tym narzędzi do współpracy i klientów VPN, które mają istotne znaczenie podczas pracy zdalnej.

Pełną listę obsługiwanych produktów innych firm przeznaczonych do systemu operacyjnego Windows można znaleźć na stronie https://kb.acronis.com/content/62853.

Obsługiwane produkty dla systemu Linux

Ocena luk w zabezpieczeniach jest obsługiwana w przypadku następujących dystrybucji i wersji systemu Linux:

- Virtuozzo 7.0.11
- Virtuozzo 7.0.10 (320)
- Virtuozzo 7.0.9 (539)
- Virtuozzo 7.0.8 (524)
- CentOS 7.x
- Acronis Cyber Infrastructure 3.x
- Acronis Storage 2.4.0
- Acronis Storage 2.2.0

Ustawienia modułu Ocena luk w zabezpieczeniach

Więcej informacji na temat tworzenia planu ochrony z wykorzystaniem modułu Ocena luk w zabezpieczeniach można znaleźć w "Tworzenie planu ochrony" (s. 209). Skanowanie w celu oceny luk w zabezpieczeniach można przeprowadzać według harmonogramu lub na żądanie (przy użyciu czynności **Uruchom teraz** w planie ochrony).

W module Ocena luk w zabezpieczeniach można określić następujące ustawienia:

Elementy do skanowania

Wybierz oprogramowanie, które chcesz przeskanować pod kątem luk w zabezpieczeniach:

- Komputery z systemem Windows:
  - **Produkty firmy Microsoft**
  - **Produkty innych firm przeznaczone do systemu Windows**
    Więcej informacji o obsługiwanych produktach innych firm przeznaczonych do systemu operacyjnego Windows można znaleźć na stronie https://kb.acronis.com/content/62853.
- Komputery z systemem Linux:
  - **Skanuj pakiety systemu Linux**

Harmonogram

Zdefiniuj harmonogram, zgodnie z którym na wybranych komputerach będzie wykonywane skanowanie w celu oceny luk w zabezpieczeniach:

Zaplanuj wykonanie zadania przy użyciu następujących zdarzeń:

- **Zaplanuj według czasu** — zadanie zostanie uruchomione w określonym czasie.
- **Gdy użytkownik zaloguje się w systemie** — domyślnie zalogowanie się dowolnego użytkownika spowoduje uruchomienie zadania. Można zmodyfikować to ustawienie tak, aby zadanie było wyzwalane tylko przez określone konto użytkownika.
- **Gdy użytkownik wyloguje się z systemu** — domyślnie wylogowanie się dowolnego użytkownika spowoduje uruchomienie zadania. Można zmodyfikować to ustawienie tak, aby zadanie było wyzwalane tylko przez określone konto użytkownika.

  Uwaga
  Zadanie nie zostanie uruchomione przy zamykaniu systemu. Zamknięcie systemu i wylogowanie to różne zdarzenia w konfiguracji harmonogramu.

- **Podczas uruchamiania systemu** — zadanie zostanie uruchomione podczas uruchamiania systemu operacyjnego.
- **Podczas zamknięcia systemu** — zadanie zostanie uruchomione podczas zamykania systemu operacyjnego.

Ustawienie domyślne: **Zaplanuj według czasu**.

Typ harmonogramu:

- **Co miesiąc** — należy wybrać miesiące i tygodnie lub dni miesiąca, w których zadanie będzie uruchamiane.
- **Codziennie** — należy wybrać dni tygodnia, w których zadanie będzie uruchamiane.
- **Co godzinę** — należy wybrać dni tygodnia, liczbę powtórzeń oraz przedział czasu, w których zadanie będzie uruchamiane.

Ustawienie domyślne: **Codziennie**.

Rozpocznij o — należy wybrać dokładną godzinę, o której zadanie zostanie uruchomione.

Uruchom w podanym okresie — należy ustawić zakres czasu, w którym będzie obowiązywać skonfigurowany harmonogram.

Warunki uruchomienia — należy określić wszystkie warunki, które muszą być jednocześnie spełnione, aby zostało uruchomione zadanie.

Warunki uruchomienia skanowania pod kątem złośliwego oprogramowania są podobne do warunków uruchomienia modułu Kopia zapasowa, które opisano w "Warunki rozpoczęcia" (s. 248). Można zdefiniować następujące dodatkowe warunki uruchomienia:

- **Rozłóż rozpoczęcie zadania w przedziale czasu** — ta opcja umożliwia zdefiniowanie ram czasowych zadań, aby uniknąć wąskich gardeł na łączach sieciowych. Możesz określić opóźnienie w godzinach lub minutach. Jeśli na przykład domyślną godziną rozpoczęcia jest 10:00, a opóźnienie wynosi 60 minut, to zadanie rozpocznie się między godziną 10:00 a 11:00.
- **Jeśli komputer jest wyłączony, uruchom pominięte zadania przy jego uruchamianiu**
- **Zablokuj włączanie trybu uśpienia lub hibernacji podczas wykonywania zadania** — ta opcja działa tylko w przypadku komputerów z systemem Windows.
- **Nawet jeśli warunki uruchomienia nie są spełnione, wykonaj zadanie po** — określ czas, po którym zadanie zostanie uruchomione, bez względu na spełnienie innych warunków rozpoczęcia.

Uwaga
Warunki uruchomienia nie są obsługiwane w systemie Linux.

Ocena luk w zabezpieczeniach komputerów z systemem Windows

Komputery z systemem Windows i produktami innych firm dla systemu Windows można skanować w poszukiwaniu luk w zabezpieczeniach.

1. W konsoli internetowej Cyber Protect utwórz plan ochrony i włącz moduł **Ocena luk w zabezpieczeniach**.
2. Określ ustawienia oceny luk w zabezpieczeniach:
   - **Elementy do skanowania** — zaznacz **Produkty firmy Microsoft**, **Produkty firmy Microsoft, produkty innych firm przeznaczone do systemu Windows** lub obie te opcje.
   - **Harmonogram** — określ harmonogram przeprowadzania ocen luk w zabezpieczeniach. Dodatkowe informacje na temat opcji **Harmonogram** można znaleźć w "Ustawienia modułu Ocena luk w zabezpieczeniach" (s. 558).
3. Przypisz plan do komputerów z systemem Windows.

Po przeprowadzeniu skanowania w celu oceny luk w zabezpieczeniach możesz sprawdzić listę znalezionych luk. Możesz przeanalizować te informacje i zdecydować, które luki w zabezpieczeniach muszą zostać usunięte.

Aby monitorować wyniki skanowania w celu oceny luk w zabezpieczeniach, skorzystaj z widżetów **Pulpit nawigacyjny** > **Przegląd** > **Luki w zabezpieczeniach / Występujące luki w zabezpieczeniach**.

Ocena luk w zabezpieczeniach w przypadku komputerów z systemem Linux

Możesz skanować komputery z systemem Linux w poszukiwaniu luk w zabezpieczeniach na poziomie aplikacji i jądra.

Aby skonfigurować ocenę luk w zabezpieczeniach w przypadku komputerów z systemem Linux

1. W konsoli internetowej Cyber Protect utwórz plan ochrony i włącz moduł **Ocena luk w zabezpieczeniach**.
2. Określ ustawienia oceny luk w zabezpieczeniach:
   - **Elementy do skanowania** — wybierz **Skanuj pakiety systemu Linux**.
   - **Harmonogram** — określ harmonogram przeprowadzania ocen luk w zabezpieczeniach. Dodatkowe informacje na temat opcji **Harmonogram** można znaleźć w "Ustawienia modułu Ocena luk w zabezpieczeniach" (s. 558).
3. Przypisz plan do komputerów z systemem Linux.

Po przeprowadzeniu skanowania w celu oceny luk w zabezpieczeniach możesz sprawdzić listę znalezionych luk. Możesz przeanalizować te informacje i zdecydować, które luki w zabezpieczeniach muszą zostać usunięte.

Aby monitorować wyniki skanowania w celu oceny luk w zabezpieczeniach, skorzystaj z widżetów **Pulpit nawigacyjny** > **Przegląd** > **Luki w zabezpieczeniach / Występujące luki w zabezpieczeniach**.

Zarządzanie znalezionymi lukami w zabezpieczeniach

Jeśli choć raz wykonano ocenę luk w zabezpieczeniach i wykryto jakieś luki, będą one widoczne w sekcji **Zarządzanie oprogramowaniem** > **Luki w zabezpieczeniach**. Na liście luk w zabezpieczeniach są pokazywane zarówno luki, w których przypadku są dostępne poprawki, jak i te, dla których nie ma proponowanych poprawek. Korzystając z filtru, można wyświetlić tylko luki z dostępnymi poprawkami.

Nazwa	Opis
Nazwa	Nazwa luki w zabezpieczeniach.
Produkty dotknięte problemem	Programy, w których wykryto luki.
Komputery	Liczba komputerów dotkniętych problemem.
Ważność	Ważność znalezionej luki. Może to być jeden z następujących poziomów ważności określony zgodnie z

	systemem Common Vulnerability Scoring System (CVSS): • **Krytyczny**: 9–10 w skali CVSS • **Wysoki**: 7–9 w skali CVSS • **Średni**: 3–7 w skali CVSS • **Niski**: 0–3 w skali CVSS • **Brak**
Poprawki	Liczba odpowiednich poprawek.
Opublikowano	Data i godzina opublikowania luki w zabezpieczeniach na liście Common Vulnerabilities and Exposures (CVE).
Wykryto	Dzień pierwszego wykrycia danej luki na komputerach.

Opis znalezionej luki w zabezpieczeniach można wyświetlić przez kliknięcie jej nazwy na liście.

Aby rozpocząć naprawianie luk w zabezpieczeniach

1. W konsoli internetowej Cyber Protect przejdź do sekcji **Zarządzanie oprogramowaniem** > **Luki w zabezpieczeniach**.
2. Wybierz luki z listy, a następnie kliknij **Zainstaluj poprawki**. Zostanie otwarty kreator naprawy luk w zabezpieczeniach.
3. Wybierz poprawki do zainstalowania. Kliknij **Dalej**.
4. Wybierz komputery, na których chcesz zainstalować poprawki.
5. Określ, czy po zainstalowaniu poprawek komputery mają zostać uruchomione ponownie:
   - **Nie** — po instalacji poprawki nie będzie inicjowane ponowne uruchomienie.
   - **Jeśli jest to wymagane** — ponowne uruchomienie jest inicjowane tylko wtedy, gdy jest niezbędne do zastosowania aktualizacji.
   - **Tak** — po instalacji poprawki zawsze zostanie zainicjowane ponowne uruchomienie. Można jednak określić opóźnienie.

   Nie uruchamiaj ponownie, dopóki nie zakończy się tworzenie kopii zapasowej — w przypadku działania procesu tworzenia kopii zapasowej ponowne uruchomienie komputera zostanie opóźnione do czasu zakończenia operacji tworzenia kopii zapasowej.
6. Kliknij **Zainstaluj poprawki**.

W wyniku tego na wybranych komputerach zostaną zainstalowane wybrane poprawki.

Zarządzanie poprawkami

Funkcja zarządzania poprawkami umożliwia:

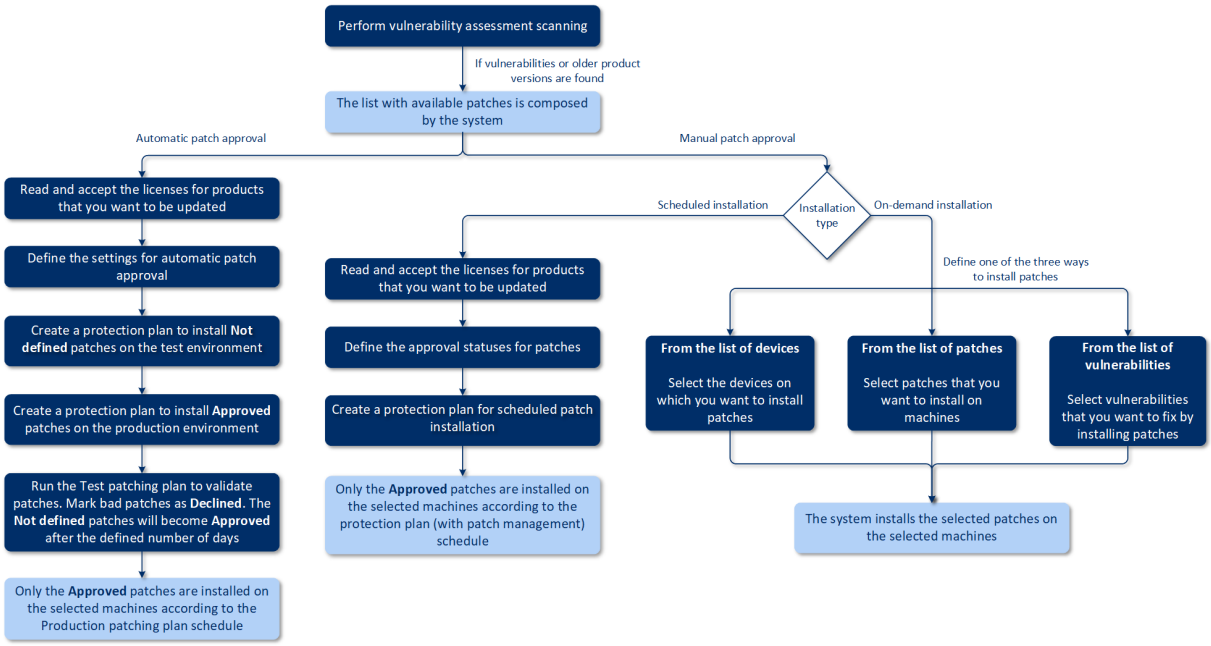
- Instalowanie aktualizacji na poziomie systemu operacyjnego i aplikacji
- Ręczne lub automatyczne zatwierdzanie poprawek
- Instalowanie poprawek na żądanie i zgodnie z harmonogramem

- Dokładne określanie, które poprawki mają zostać zastosowane, przy użyciu różnych kryteriów: ważność, kategoria i status zatwierdzenia
- Tworzenie kopii zapasowych przed zainstalowaniem aktualizacji, aby zapobiec ewentualnym nieudanym aktualizacjom
- Wybór opcji ponownego uruchomienia, która ma być stosowana po zainstalowaniu poprawki

Aby zminimalizować ruch w sieci, usługa Cyber Protect stosuje technologię komunikacji peer-to-peer. Możesz wybrać specjalne agenty, które będą pobierać aktualizacje z Internetu i je rozpowszechniać wśród innych agentów w sieci. Wszystkie agenty będą też udostępniać sobie nawzajem aktualizacje jako agenty peer-to-peer.

Sposób działania

Możesz skonfigurować automatyczne lub ręczne zatwierdzanie poprawek. Na poniższym schemacie widać zarówno automatyczne, jak i ręczne procesy zatwierdzania poprawek.



1. Najpierw trzeba wykonać co najmniej jedno skanowanie w celu oceny luk w zabezpieczeniach przy użyciu planu ochrony z włączonym modułem **Ocena luk w zabezpieczeniach**. Po zakończeniu skanowania system tworzy listy znalezionych luk w zabezpieczeniach i dostępnych poprawek.
2. Następnie można skonfigurować automatyczne zatwierdzanie poprawek lub zdecydować się na ręczne zatwierdzanie poprawek.
3. Wskaż, jak mają być instalowane poprawki — zgodnie z harmonogramem czy na żądanie. Instalowanie poprawek na żądanie może być wykonane na trzy sposoby, zgodnie z Twoimi preferencjami:
   - Przejdź do listy poprawek (**Zarządzanie oprogramowaniem** > **Poprawki**) i zainstaluj niezbędne poprawki.

- Przejdź do listy luk w zabezpieczeniach (**Zarządzanie oprogramowaniem** > **Luki w zabezpieczeniach**) i rozpocznij proces naprawy, który obejmuje również instalację poprawek.
- Przejdź do listy urządzeń (**Urządzenia**> **Wszystkie urządzenia**), wybierz komputery, które chcesz zaktualizować, i zainstaluj na nich poprawki.

Wyniki instalacji poprawek można monitorować w widżecie **Pulpit nawigacyjny** > **Przegląd** > **Historia instalacji poprawek**.

Ustawienia modułu Zarządzanie poprawkami

Więcej informacji na temat tworzenia planu ochrony z wykorzystaniem modułu Zarządzanie poprawkami można znaleźć w sekcji „Tworzenie planu ochrony". Za pomocą planu ochrony można określić, jakie aktualizacje produktów firmy Microsoft i innych firm przeznaczonych do systemu Windows mają być automatycznie instalowane na wskazanych komputerach.

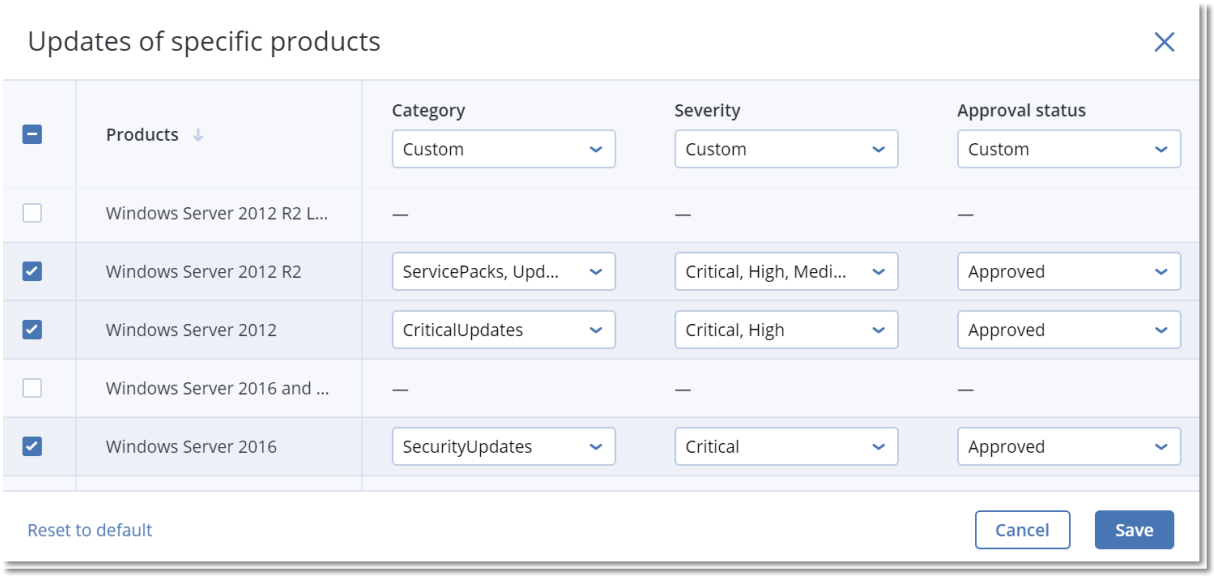
W przypadku modułu Zarządzanie poprawkami można określić następujące ustawienia.

Produkty firmy Microsoft

Aby zainstalować aktualizacje firmy Microsoft na wybranych komputerach, włącz opcję **Aktualizuj produkty firmy Microsoft**.

Wybierz aktualizacje, które chcesz instalować:

- **Wszystkie aktualizacje**
- **Tylko aktualizacje zabezpieczeń i aktualizacje krytyczne**
- **Aktualizacje określonych produktów** — można zdefiniować niestandardowe ustawienia dla różnych produktów. Jeśli chcesz zaktualizować określone produkty, w przypadku każdego z nich możesz zdefiniować, które aktualizacje mają zostać zainstalowane, na podstawie kategorii, ważności lub statusu zatwierdzenia.

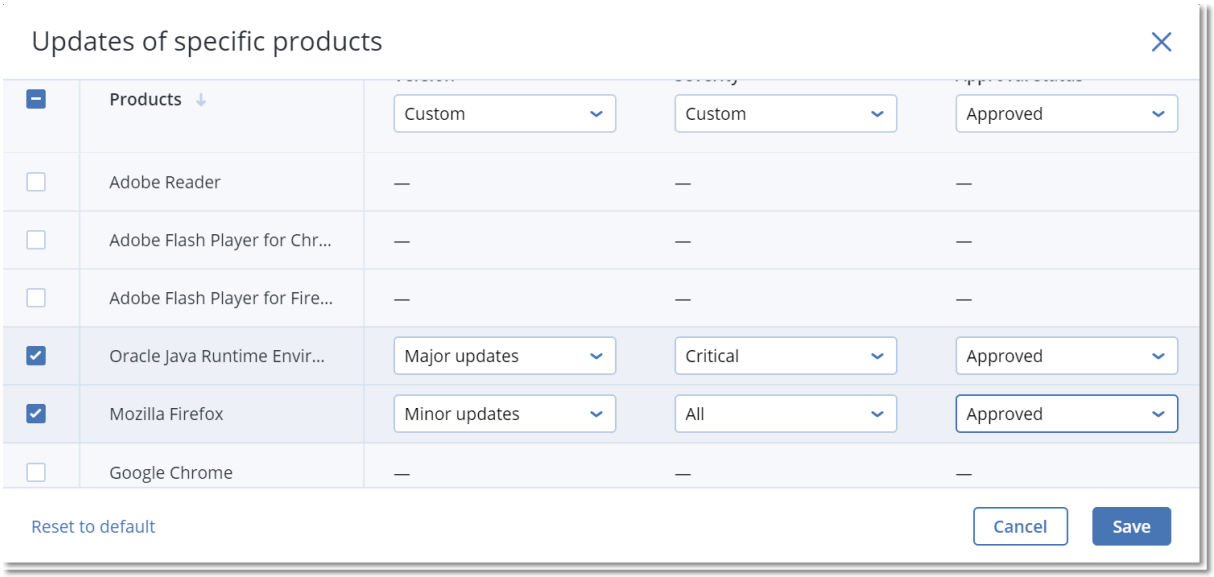


Produkty innych firm przeznaczone do systemu Windows

Aby zainstalować aktualizacje produktów innych firm przeznaczonych do systemu Windows na wybranych komputerach, włącz opcję **Produkty innych firm przeznaczone do systemu Windows**.

Wybierz aktualizacje, które chcesz instalować:

- **Tylko ważne aktualizacje** — umożliwia zainstalowanie najnowszej dostępnej wersji aktualizacji.
- **Tylko drobne aktualizacje** — umożliwia zainstalowanie wersji pomocniczej aktualizacji.
- **Aktualizacje określonych produktów** — można zdefiniować niestandardowe ustawienia dla różnych produktów. Jeśli chcesz zaktualizować określone produkty, w przypadku każdego z nich możesz zdefiniować, które aktualizacje mają zostać zainstalowane, na podstawie kategorii, ważności lub statusu zatwierdzenia.



Harmonogram

Zdefiniuj harmonogram, zgodnie z którym na wybranych komputerach będą instalowane aktualizacje.

Zaplanuj wykonanie zadania przy użyciu następujących zdarzeń:

- **Zaplanuj według czasu** — zadanie zostanie uruchomione w określonym czasie.
- **Gdy użytkownik zaloguje się w systemie** — domyślnie zalogowanie się dowolnego użytkownika spowoduje uruchomienie zadania. Można zmodyfikować to ustawienie tak, aby zadanie było wyzwalane tylko przez określone konto użytkownika.
- **Gdy użytkownik wyloguje się z systemu** — domyślnie wylogowanie się dowolnego użytkownika spowoduje uruchomienie zadania. Można zmodyfikować to ustawienie tak, aby zadanie było wyzwalane tylko przez określone konto użytkownika.

Uwaga
Zadanie nie zostanie uruchomione przy zamykaniu systemu. Zamknięcie systemu i wylogowanie to różne zdarzenia w konfiguracji harmonogramu.

- **Podczas uruchamiania systemu** — zadanie zostanie uruchomione podczas uruchamiania systemu operacyjnego.
- **Podczas zamknięcia systemu** — zadanie zostanie uruchomione podczas zamykania systemu operacyjnego.

Ustawienie domyślne: **Zaplanuj według czasu**.

Typ harmonogramu:

- **Co miesiąc** — należy wybrać miesiące i tygodnie lub dni miesiąca, w których zadanie będzie uruchamiane.
- **Codziennie** — należy wybrać dni tygodnia, w których zadanie będzie uruchamiane.
- **Co godzinę** — należy wybrać dni tygodnia, liczbę powtórzeń oraz przedział czasu, w których zadanie będzie uruchamiane.

Ustawienie domyślne: **Codziennie**.

Rozpocznij o — należy wybrać dokładną godzinę, o której zadanie zostanie uruchomione.

Uruchom w podanym okresie — należy ustawić zakres czasu, w którym będzie obowiązywać skonfigurowany harmonogram.

Warunki uruchomienia — należy określić wszystkie warunki, które muszą być jednocześnie spełnione, aby zostało uruchomione zadanie.

Warunki uruchomienia skanowania pod kątem złośliwego oprogramowania są podobne do warunków uruchomienia modułu Kopia zapasowa, które opisano w "Warunki rozpoczęcia" (s. 248). Można zdefiniować następujące dodatkowe warunki uruchomienia:

- **Rozłóż rozpoczęcie zadania w przedziale czasu** — ta opcja umożliwia zdefiniowanie ram czasowych zadań, aby uniknąć wąskich gardeł na łączach sieciowych. Możesz określić opóźnienie w godzinach lub minutach. Jeśli na przykład domyślną godziną rozpoczęcia jest 10:00, a opóźnienie wynosi 60 minut, to zadanie rozpocznie się między godziną 10:00 a 11:00.
- **Jeśli komputer jest wyłączony, uruchom pominięte zadania przy jego uruchamianiu**
- **Zablokuj włączanie trybu uśpienia lub hibernacji podczas wykonywania zadania** — ta opcja działa tylko w przypadku komputerów z systemem Windows.
- **Nawet jeśli warunki uruchomienia nie są spełnione, wykonaj zadanie po** — określ czas, po którym zadanie zostanie uruchomione, bez względu na spełnienie innych warunków rozpoczęcia.

Kopia zapasowa przed aktualizacją

Uruchom operację tworzenia kopii zapasowej przed zainstalowaniem aktualizacji oprogramowania — system utworzy przyrostową kopię zapasową komputera, zanim zostanie na

nim zainstalowana jakakolwiek aktualizacja. Jeśli jeszcze nie utworzono żadnej kopii zapasowej tego komputera, to zostanie utworzona jego pełna kopia zapasowa. W razie niepowodzenia instalacji poprawki pozwoli Ci ona wrócić do poprzedniego stanu. Aby opcja **Kopia zapasowa przed aktualizacją** zadziałała, komputery muszą mieć włączone w planie ochrony moduły Zarządzanie poprawkami i Kopia zapasowa oraz odpowiednie elementy do uwzględnienia w kopiach zapasowych — cały komputer lub wolumin rozruchowy i systemowy. W przypadku wybrania niewłaściwych elementów do uwzględnienia w kopii zapasowej, system nie umożliwi włączenia opcji **Kopia zapasowa przed aktualizacją**.

Zarządzanie listą poprawek

Po wykonaniu zakończeniu procesu oceny luk w zabezpieczeniach dostępne poprawki można znaleźć w sekcji **Zarządzanie oprogramowaniem** > **Poprawki**.

Nazwa	Opis
Nazwa	Nazwa poprawki
Ważność	Poziom ważności poprawki: • **Krytyczny** • **Wysoki** • **Średni** • **Niski** • **Brak**
Dostawca	Dostawca poprawki
Produkt	Produkt, którego dotyczy poprawka
Zainstalowane wersje	Już zainstalowane wersje produktów
Wersja	Wersja poprawki
Kategoria	Kategoria, do której należy poprawka: • **Aktualizacja krytyczna** — powszechnie udostępniane rozwiązania krytycznych, niezwiązanych z bezpieczeństwem problemów. • **Aktualizacja zabezpieczeń** — powszechnie udostępniane poprawki do określonych produktów eliminujące problemy z bezpieczeństwem. • **Aktualizacja definicji** — aktualizacje definicji wirusów lub innych plików definicji. • **Pakiet zbiorczy aktualizacji** — zbiorczy zestaw poprawek, aktualizacji zabezpieczeń, aktualizacji krytycznych i zwykłych aktualizacji zebranych w jednym pakiecie w celu łatwego wdrożenia. Pakiet zbiorczy na ogół jest ukierunkowany na konkretny obszar, np.

	bezpieczeństwo, lub konkretny komponent, np. usługi Internet Information Services (IIS). • **Dodatek Service Pack** — zbiorczy zestaw wszystkich poprawek, aktualizacji zabezpieczeń, aktualizacji krytycznych i zwykłych aktualizacji utworzonych od czasu wydania produktu. Dodatki Service Pack mogą również zawierać niewielką liczbę zmian projektowych lub funkcjonalnych wprowadzonych na życzenie klientów. • **Narzędzie** — narzędzia lub funkcje, które ułatwiają realizację zadania lub zestawu zadań. • **Pakiet funkcji** — nowe funkcje, zwykle wprowadzane do produktów w nowej wersji. • **Aktualizacja** — powszechnie udostępniane rozwiązania niekrytycznych, niezwiązanych z bezpieczeństwem problemów. • **Aplikacja** — poprawki do aplikacji.
Microsoft KB	W przypadku poprawki do produktu firmy Microsoft podawany jest identyfikator artykułu z bazy wiedzy.
Data wydania	Data wydania poprawki
Komputery	Liczba komputerów dotkniętych problemem
Status zatwierdzenia	Status zatwierdzenia jest potrzebny przede wszystkim w przypadku scenariusza automatycznego zatwierdzania oraz do wskazania w planie ochrony aktualizacji do zainstalowania — na podstawie statusu. Możesz zdefiniować jeden z poniższych statusów poprawki: • **Zatwierdzono** — poprawka została zainstalowana na co najmniej jednym komputerze i zatwierdzona jako odpowiednia • **Odmówiono** — poprawka nie jest bezpieczna i może uszkodzić system komputera • **Nie zdefiniowano** — status poprawki jest niejasny i powinien zostać zweryfikowany
Umowa licencyjna	• Przeczytaj i zaakceptuj • Odmowa akceptacji. Jeśli nie zgadzasz się na warunki umowy licencyjnej, to poprawka otrzymuje status **Odmówiono** i nie zostaje zainstalowana
Luki w zabezpieczeniach	Liczba luk w zabezpieczeniach. Jej kliknięcie spowoduje przejście do listy luk w zabezpieczeniach.

Rozmiar	Średni rozmiar poprawki
Język	Język obsługiwany przez poprawkę
Witryna dostawcy	Oficjalna witryna internetowa dostawcy poprawki

Automatyczne zatwierdzanie poprawek

Automatyczne zatwierdzanie poprawek ułatwia instalację aktualizacji na komputerach. Aby opisać, jak to działa, posłużymy się przykładem.

Sposób działania

Załóżmy, że istnieją dwa środowiska: testowe i produkcyjne. Środowisko testowe służy do testowania instalacji poprawek i sprawdzania, czy niczego nie psują. Po przetestowaniu instalacji poprawek w środowisku testowym bezpieczne poprawki mogą zostać automatycznie zainstalowane w środowisku produkcyjnym.

Konfigurowanie automatycznego zatwierdzania poprawek

Aby skonfigurować automatyczne zatwierdzanie poprawek

1. W przypadku każdego sprzedawcy, którego produkty planujesz aktualizować, musisz przeczytać i zaakceptować umowy licencyjne. W przeciwnym razie automatyczna instalacja poprawek nie będzie możliwa.
2. Skonfiguruj ustawienia automatycznego zatwierdzania.
3. Przygotuj plan ochrony (na przykład „Poprawki testowe") z włączonym modułem **Zarządzanie poprawkami** i zastosuj go do komputerów w środowisku testowym. Określ następujący warunek instalacji poprawek: status zatwierdzenia poprawki musi mieć wartość **Nie zdefiniowano**. Ten krok jest potrzebny do weryfikacji poprawek i sprawdzenia, czy komputery działają prawidłowo po ich zainstalowaniu.
4. Przygotuj plan ochrony (na przykład „Poprawki produkcyjne") z włączonym modułem **Zarządzanie poprawkami** i zastosuj go do komputerów w środowisku produkcyjnym. Określ następujący warunek instalacji poprawek: status poprawki musi mieć wartość **Zatwierdzono**.
5. Uruchom plan Poprawki testowe i sprawdź wyniki. Status zatwierdzenia w przypadku komputerów działających bez problemów można zachować jako **Nie zdefiniowano**, natomiast w przypadku komputerów działających nieprawidłowo status musi mieć wartość **Odmówiono**.
6. Zgodnie z liczbą dni ustawioną w polu opcji **Automatyczne zatwierdzanie** poprawki, które miały status **Nie zdefiniowano** otrzymają status **Zatwierdzono**.
7. Po uruchomieniu planu Poprawki produkcyjne na komputerach produkcyjnych zostaną zainstalowane tylko poprawki ze statusem **Zatwierdzono**.

Poniżej wymieniono czynności wykonywane ręcznie.

Krok 1. Przeczytaj i zaakceptuj umowy licencyjne na produkty, które chcesz zaktualizować

1. W konsoli internetowej Cyber Protect przejdź do sekcji **Zarządzanie oprogramowaniem** > **Poprawki**.
2. Wybierz poprawkę, a następnie przeczytaj i zaakceptuj umowę licencyjną.

Krok 2. Skonfiguruj ustawienia na potrzeby automatycznego zatwierdzania

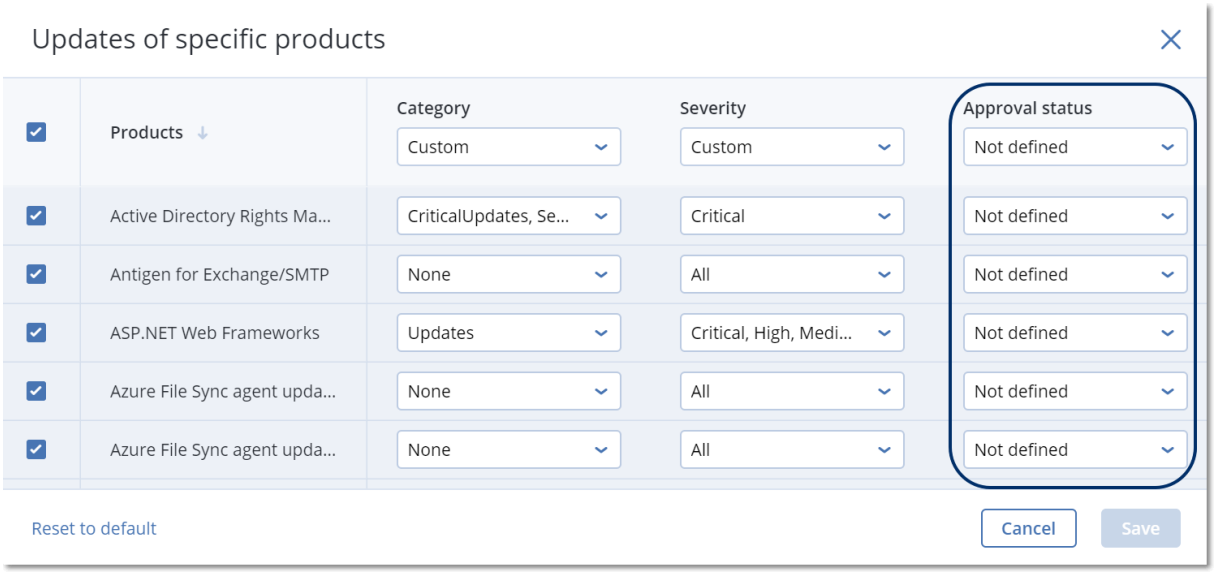
1. W konsoli internetowej Cyber Protect przejdź do sekcji **Zarządzanie oprogramowaniem** > **Poprawki**.
2. Kliknij **Ustawienia**.
3. Włącz opcję **Automatyczne zatwierdzanie** i podaj liczbę dni. Oznacza to, że po upływie określonej liczby dni od pierwszej próby instalacji poprawek poprawki ze statusem **Nie zdefiniowano** automatycznie otrzymają status **Zatwierdzono**.

   Załóżmy na przykład, że określono 10 dni. Wykonano plan Poprawki testowe na komputerach testowych i zainstalowano poprawki. Poprawki, które coś popsuły na komputerach, oznaczono statusem **Odmówiono**, a resztę poprawek — statusem **Nie zdefiniowano**. 10 dni później poprawki ze statusem **Nie zdefiniowano** automatycznie otrzymały status **Zatwierdzono**.
4. Włącz opcję **Automatycznie zaakceptuj umowy licencyjne**. Jest to potrzebne do automatycznej akceptacji licencji podczas instalacji poprawki — tak aby nie było wymagane potwierdzenie od użytkownika.

Krok 3. Przygotuj plan ochrony Poprawki testowe

1. W konsoli internetowej Cyber Protect przejdź do sekcji **Plany** > **Ochrona**.
2. Kliknij **Utwórz plan**.
3. Włącz moduł **Zarządzanie poprawkami**.
4. Określ, które aktualizacje produktów firmy Microsoft i innych firm mają zostać zainstalowane, zaplanuj tę operację w harmonogramie i utwórz kopię zapasową przed aktualizacją. Więcej informacji na temat tych ustawień można znaleźć w sekcji „Ustawienia modułu Zarządzanie poprawkami”.

Ważne
W przypadku wszystkich aktualizowanych produktów należy określić **Status zatwierdzenia** jako **Nie zdefiniowano**. Gdy przyjdzie czas na aktualizację, agent zainstaluje tylko poprawki ze statusem **Nie zdefiniowano** na wybranych komputerach w środowisku testowym.

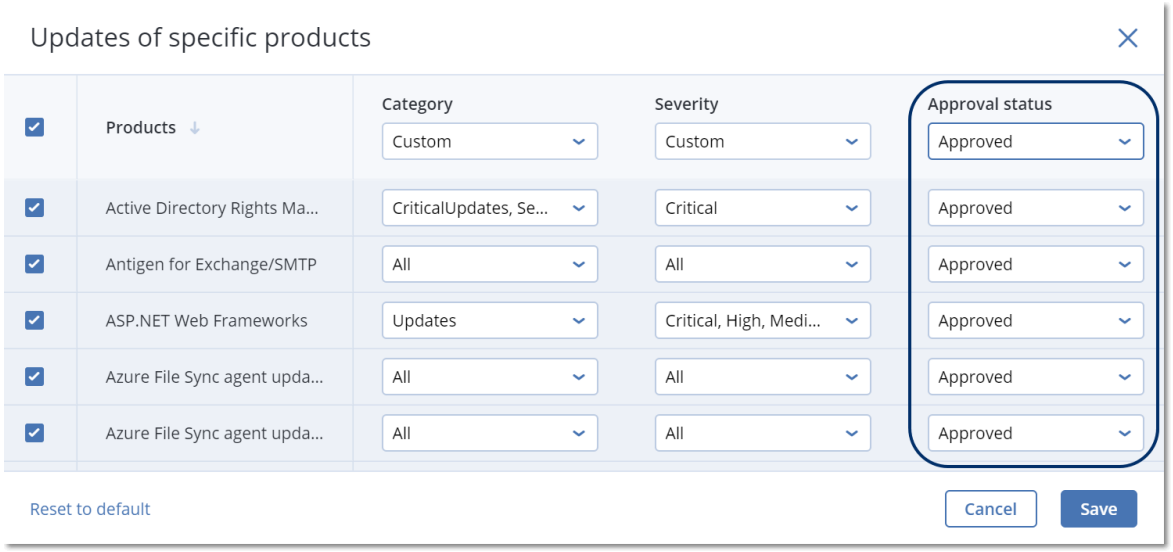


Krok 4. Przygotuj plan ochrony Poprawki produkcyjne

1. W konsoli internetowej Cyber Protect przejdź do sekcji **Plany** > **Ochrona**.
2. Kliknij **Utwórz plan**.
3. Włącz moduł **Zarządzanie poprawkami**.
4. Określ, które aktualizacje produktów firmy Microsoft i innych firm mają zostać zainstalowane, zaplanuj tę operację w harmonogramie i utwórz kopię zapasową przed aktualizacją. Więcej informacji na temat tych ustawień można znaleźć w sekcji „Ustawienia modułu Zarządzanie poprawkami”.

Ważne
W przypadku wszystkich aktualizowanych produktów należy określić **Status zatwierdzenia** jako **Zatwierdzono**. Gdy przyjdzie czas na aktualizację, agent zainstaluje tylko poprawki ze statusem **Zatwierdzono** na wybranych komputerach w środowisku produkcyjnym.

Uwaga



Krok 5. Uruchom plan ochrony Poprawki testowe i sprawdź wyniki

1. Uruchom plan ochrony Poprawki testowe (według harmonogramu lub na żądanie).
2. Następnie sprawdź, które z zainstalowanych poprawek są bezpieczne, a które nie.
3. Przejdź do sekcji **Zarządzanie oprogramowaniem** > **Poprawki** i w przypadku poprawek, które nie są bezpieczne, ustaw **Status zatwierdzenia** jako **Odmówiono**.

Ręczne zatwierdzanie poprawek

Proces ręcznego zatwierdzania poprawek przebiega następująco:

1. W konsoli internetowej Cyber Protect przejdź do sekcji **Zarządzanie oprogramowaniem** > **Poprawki**.
2. Wybierz poprawki do zainstalowania, a następnie przeczytaj i zaakceptuj umowy licencyjne.
3. Ustaw **Status zatwierdzenia** poprawek, które chcesz zainstalować, jako **Zatwierdzono**.
4. Utwórz plan ochrony z włączonym modułem Zarządzanie poprawkami. Możesz skonfigurować harmonogram lub uruchomić plan na żądanie, klikając **Uruchom teraz** w ustawieniach modułu Zarządzanie poprawkami.

W wyniku tego na wybranych komputerach zostaną zainstalowane tylko zatwierdzone poprawki.

Instalacja poprawek na żądanie

Instalowanie poprawek na żądanie może być wykonane na trzy sposoby, zgodnie z Twoimi preferencjami:

- Przejdź do listy poprawek (**Zarządzanie oprogramowaniem** > **Poprawki**) i zainstaluj niezbędne poprawki.

- Przejdź do listy luk w zabezpieczeniach (**Zarządzanie oprogramowaniem** > **Luki w zabezpieczeniach**) i rozpocznij proces naprawy, który obejmuje również instalację poprawek.
- Przejdź do listy urządzeń (**Urządzenia**> **Wszystkie urządzenia**), wybierz komputery, które chcesz zaktualizować, i zainstaluj na nich poprawki.

Rozważmy instalację poprawek z listy poprawek:

1. W konsoli internetowej Cyber Protect przejdź do sekcji **Zarządzanie oprogramowaniem** > **Poprawki**.
2. Zaakceptuj umowy licencyjne poprawek, które chcesz zainstalować.
3. Wybierz poprawki, które chcesz zainstalować, i kliknij **Zainstaluj**.
4. Wybierz komputery, na których muszą zostać zainstalowane poprawki.
5. Określ, czy po zainstalowaniu poprawki zostanie zainicjowane ponowne uruchomienie:
   - **Nigdy** — po instalacji poprawki nigdy nie będzie inicjowane ponowne uruchomienie.
   - **Jeśli jest to wymagane** — ponowne uruchomienie jest wykonywane tylko wtedy, gdy jest niezbędne do zastosowania poprawki.
   - **Zawsze** — po instalacji poprawki zawsze zostanie zainicjowane ponowne uruchomienie. Zawsze można zdefiniować opóźnienie ponownego uruchomienia.

   Nie uruchamiaj ponownie, dopóki nie zakończy się tworzenie kopii zapasowej — w przypadku działania procesu tworzenia kopii zapasowej ponowne uruchomienie komputera zostanie opóźnione do czasu zakończenia operacji tworzenia kopii zapasowej.
6. Kliknij **Zainstaluj poprawki**.

Na wybranych komputerach zostaną zainstalowane wybrane poprawki.

Czas występowania poprawki na liście

Aby zadbać o aktualność listy poprawek, przejdź do sekcji **Zarządzanie oprogramowaniem** > **Poprawki** > **Ustawienia** i określ opcję **Czas występowania na liście**.

Opcja **Czas występowania na liście** określa, jak długo wykryta dostępna poprawka będzie się znajdowała na liście poprawek. Ogólnie rzecz biorąc, poprawka zostanie usunięta z listy, gdy zostanie pomyślnie zainstalowana na wszystkich komputerach, na których wykryto jej brak, albo po upływie określonego czasu.

- **Bezterminowo** — poprawka będzie się znajdować na liście przez cały czas.
- **7 dni** — poprawka zostanie usunięta po 7 dniach od jej pierwszej instalacji.
  Załóżmy na przykład, że masz dwa komputery, na których muszą zostać zainstalowane poprawki. Jeden z nich działa w trybie online, drugi — offline. Poprawka została zainstalowana na pierwszym komputerze. Po 7 dniach poprawka zostanie usunięta z listy poprawek, nawet jeśli nie została zainstalowana na drugim komputerze, ponieważ był on w trybie offline.
- **30 dni** — poprawka zostanie usunięta po 30 dniach od jej pierwszej instalacji.

Inteligentna ochrona

Kanał dotyczący zagrożeń

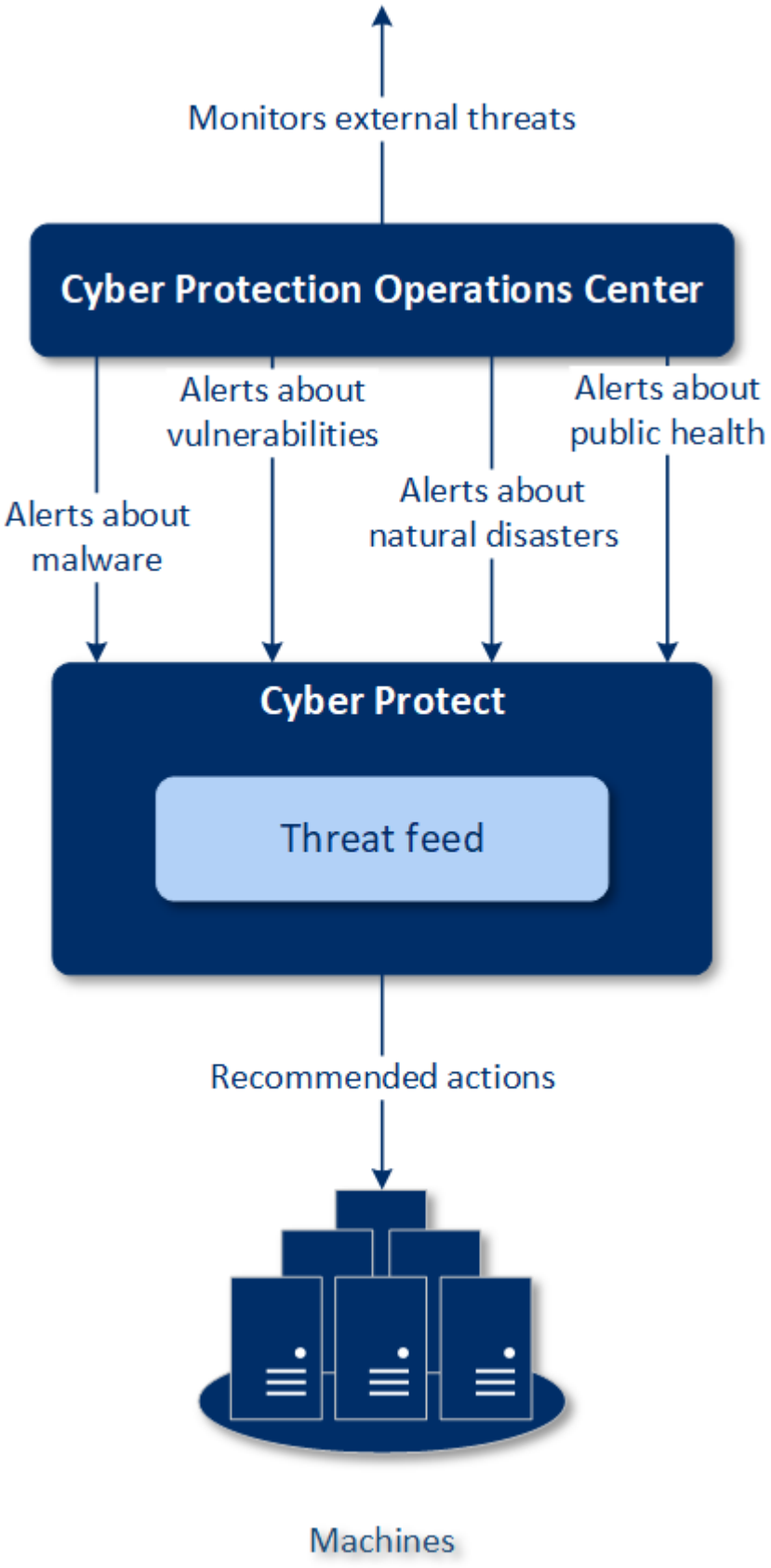
Acronis Cyber Protection Operations Center (CPOC) generuje alerty bezpieczeństwa i wysyła je tylko do tych regionów geograficznych, których te alerty dotyczą. Alerty zawierają informacje o złośliwym oprogramowaniu, lukach w zabezpieczeniach, klęskach żywiołowych, zagrożeniach zdrowia publicznego i innych rodzajach zdarzeń globalnych, które mogą mieć wpływ na ochronę Twoich danych. Kanał dotyczący zagrożeń zawiera informacje o wszelkich potencjalnych zagrożeniach i pozwala im zapobiegać.

Problem sygnalizowany przez alert bezpieczeństwa może zostać rozwiązany za pomocą pewnych konkretnych działań podejmowanych przez ekspertów ds. bezpieczeństwa. Niektóre alerty są tylko źródłem informacji o nadchodzących zagrożeniach — nie ma w ich przypadku żadnych zalecanych działań.

Sposób działania

Acronis Cyber Protection Operations Center monitoruje zewnętrzne zagrożenia i generuje alerty o złośliwym oprogramowaniu, lukach w zabezpieczeniach, zagrożeniach klęskami żywiołowymi i zagrożeniach zdrowia publicznego. Wszystkie te alerty będą widoczne w konsoli internetowej Cyber Protect — w sekcji **Kanał dotyczący zagrożeń**. W zależności od rodzaju alertu można podjąć odpowiednie zalecane działania.

Na poniższym schemacie przedstawiono główny przepływ roboczy kanału dotyczącego zagrożeń.



Aby wykonać zalecane działania w przypadku otrzymanych alertów z Acronis Cyber Protection Operations Center:

1. W konsoli internetowej Cyber Protect przejdź do sekcji **Panele** > **Kanał dotyczący zagrożeń** i sprawdź ewentualne alerty bezpieczeństwa.

2. Wybierz alert z listy i zapoznaj się z jego szczegółami.

3. Kliknij **Rozpocznij**, aby uruchomić kreator.

4. Włącz opcje działań do wykonania i wybierz komputery, do których te działania mają być stosowane. Mogą zostać zaproponowane następujące działania:

- **Ocena luk w zabezpieczeniach** — przeskanowanie wybranych komputerów pod kątem luk w zabezpieczeniach
- **Zarządzanie poprawkami** — zainstalowanie poprawek na wybranych komputerach
- **Ochrona antywirusowa** — przeprowadzenie pełnego skanowania wybranych komputerów
- **Twórz kopie zapasowe chronionych lub niechronionych komputerów** — utworzenie kopii zapasowych chronionych/niechronionych komputerów

5. Kliknij **Rozpocznij**.

6. Na stronie **Działania** sprawdź, czy dane działanie zostało pomyślnie wykonane.

Usuwanie wszystkich alertów

Alerty na kanale dotyczącym zagrożeń są automatycznie czyszczone po upływie następujących okresów:

- Katastrofa naturalna — 1 tydzień
- Luka w zabezpieczeniach — 1 miesiąc
- Złośliwe oprogramowanie — 1 miesiąc
- Zdrowie publiczne — tydzień 1

Mapa ochrony danych

Funkcja Mapa ochrony danych umożliwia:

- Dostęp do szczegółowych informacji na temat przechowywanych na Twoich komputerach danych (klasyfikacja, lokalizacja, status ochrony i dodatkowe informacje).
- Wykrywanie, czy dane są chronione. Dane są uznawane za chronione, jeśli są uwzględniane w tworzonych kopiach zapasowych (plan ochrony przy włączonym module Kopia zapasowa).
- Wykonywanie działań zapewniających ochronę danych.

Sposób działania

1. Najpierw tworzysz plan ochrony przy włączonym module Mapa ochrony danych.
2. Po wykonaniu planu oraz wykryciu i przeanalizowaniu danych uzyskujesz wizualną reprezentację ochrony danych w widżecie Mapa ochrony danych.
3. Możesz też przejść do sekcji **Urządzenia** > **Mapa ochrony danych** i znaleźć tam informacje o niechronionych plikach na poszczególnych urządzeniach.
4. Można podjąć działania w celu ochrony wykrytych niechronionych plików na urządzeniach.

Zarządzanie wykrytymi niechronionymi plikami

Aby chronić ważne pliki, które zostały wykryte jako niechronione:

1. W konsoli internetowej Cyber Protect przejdź do sekcji **Urządzenia** > **Mapa ochrony danych**.
   Na liście urządzeń są dostępne ogólne informacje o liczbie niechronionych plików, rozmiarze takich plików na poszczególnych urządzeniach oraz o ostatniej operacji wykrywania danych.
   Aby chronić pliki na danym komputerze, kliknij ikonę wielokropka (...), a następnie kliknij **Chroń wszystkie pliki**. Nastąpi przekierowanie do listy planów, gdzie możesz utworzyć plan ochrony przy włączonym module Kopia zapasowa.
   Aby usunąć z listy określone urządzenie z niechronionymi plikami, kliknij **Ukryj do następnego wykrywania danych**.
2. Aby wyświetlić szczegółowe informacje o niechronionych plikach na danym urządzeniu, kliknij jego nazwę.
   Zobaczysz listę niechronionych plików z podziałem według ich rozszerzeń nazw i lokalizacji. Listę tę można filtrować według rozszerzeń.
3. Aby objąć ochroną wszystkie niechronione pliki, kliknij **Chroń wszystkie pliki**. Nastąpi przekierowanie do listy planów, gdzie możesz utworzyć plan ochrony przy włączonym module Kopia zapasowa.

Aby uzyskać informacje o niechronionych plikach w formie raportu, kliknij **Pobierz szczegółowy raport w formacie CSV**.

Ustawienia modułu Mapa ochrony danych

Więcej informacji na temat tworzenia planu ochrony z wykorzystaniem modułu Mapa ochrony danych można znaleźć w sekcji „Tworzenie planu ochrony".

W przypadku modułu Mapa ochrony danych można określić następujące ustawienia.

Harmonogram

Możesz zdefiniować różne ustawienia w celu utworzenia harmonogramu, według którego będzie wykonywane zadanie Mapy ochrony danych.

Zaplanuj wykonanie zadania przy użyciu następujących zdarzeń:

- **Zaplanuj według czasu** — zadanie zostanie uruchomione w określonym czasie.
- **Gdy użytkownik zaloguje się w systemie** — domyślnie zalogowanie się dowolnego użytkownika spowoduje uruchomienie zadania. Można zmodyfikować to ustawienie tak, aby zadanie było wyzwalane tylko przez określone konto użytkownika.
- **Gdy użytkownik wyloguje się z systemu** — domyślnie wylogowanie się dowolnego użytkownika spowoduje uruchomienie zadania. Można zmodyfikować to ustawienie tak, aby zadanie było wyzwalane tylko przez określone konto użytkownika.

Uwaga
Zadanie nie zostanie uruchomione przy zamykaniu systemu. Zamknięcie systemu i wylogowanie to różne zdarzenia w konfiguracji harmonogramu.

- **Podczas uruchamiania systemu** — zadanie zostanie uruchomione podczas uruchamiania systemu operacyjnego.
- **Podczas zamknięcia systemu** — zadanie zostanie uruchomione podczas zamykania systemu operacyjnego.

Ustawienie domyślne: **Zaplanuj według czasu**.

Typ harmonogramu:

- **Co miesiąc** — należy wybrać miesiące i tygodnie lub dni miesiąca, w których zadanie będzie uruchamiane.
- **Codziennie** — należy wybrać dni tygodnia, w których zadanie będzie uruchamiane.
- **Co godzinę** — należy wybrać dni tygodnia, liczbę powtórzeń oraz przedział czasu, w których zadanie będzie uruchamiane.

Ustawienie domyślne: **Codziennie**.

Rozpocznij o — należy wybrać dokładną godzinę, o której zadanie zostanie uruchomione.

Uruchom w podanym okresie — należy ustawić zakres czasu, w którym będzie obowiązywać skonfigurowany harmonogram.

Warunki uruchomienia — należy określić wszystkie warunki, które muszą być jednocześnie spełnione, aby zostało uruchomione zadanie.

Warunki uruchomienia skanowania pod kątem złośliwego oprogramowania są podobne do warunków uruchomienia modułu Kopia zapasowa, które opisano w "Warunki rozpoczęcia" (s. 248). Można zdefiniować następujące dodatkowe warunki uruchomienia:

- **Rozłóż rozpoczęcie zadania w przedziale czasu** — ta opcja umożliwia zdefiniowanie ram czasowych zadań, aby uniknąć wąskich gardeł na łączach sieciowych. Możesz określić opóźnienie w godzinach lub minutach. Jeśli na przykład domyślną godziną rozpoczęcia jest 10:00, a opóźnienie wynosi 60 minut, to zadanie rozpocznie się między godziną 10:00 a 11:00.
- **Jeśli komputer jest wyłączony, uruchom pominięte zadania przy jego uruchamianiu**

- **Zablokuj włączanie trybu uśpienia lub hibernacji podczas wykonywania zadania** — ta opcja działa tylko w przypadku komputerów z systemem Windows.
- **Nawet jeśli warunki uruchomienia nie są spełnione, wykonaj zadanie po** — określ czas, po którym zadanie zostanie uruchomione, bez względu na spełnienie innych warunków rozpoczęcia.

Reguły dotyczące rozszerzeń i wyjątków

Na karcie **Rozszerzenia** możesz utworzyć listę rozszerzeń plików, które będą uznawane za ważne podczas wykrywania danych i sprawdzane pod kątem statusu ochrony. Podaj rozszerzenia w następującym formacie:

```
.html, .7z, .docx, .zip, .pptx, .xml
```

Na karcie **Reguły wyjątków** możesz wskazać pliki i foldery, których statusy ochrony nie będą sprawdzane podczas wykrywania danych.

- **Ukryte pliki i foldery** — w przypadku wybrania tej opcji ukryte pliki i foldery będą pomijane podczas badania danych.
- **Pliki i foldery systemowe** — w przypadku wybrania tej opcji pliki i foldery systemowe będą pomijane podczas badania danych.

Dostęp przy użyciu pulpitu zdalnego

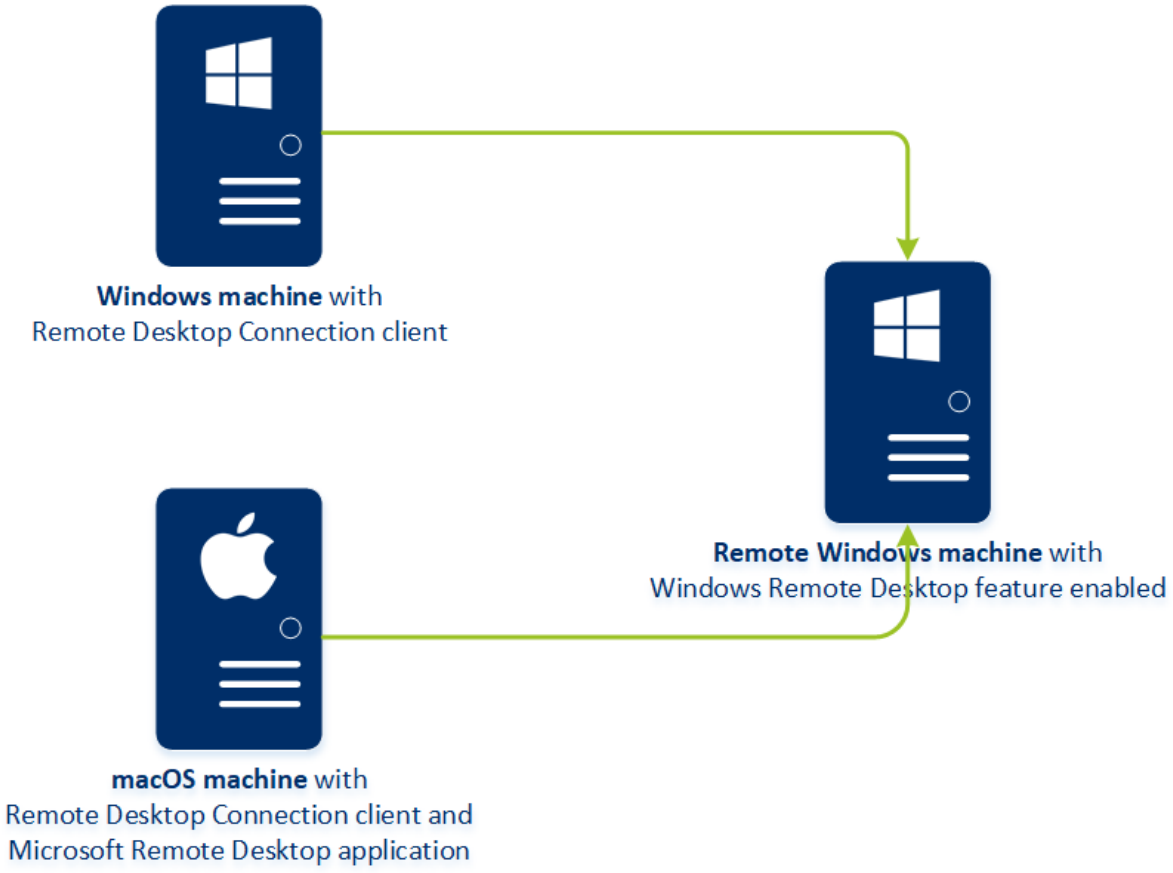
Dostęp zdalny (klienty RDP i HTML5)

Usługa Cyber Protect umożliwia dostęp zdalny. Z konsoli internetowej można zdalnie się łączyć z komputerami użytkowników i nimi zarządzać. Pozwala to na łatwe pomaganie użytkownikom w rozwiązywaniu problemów na ich komputerach.

Wymagania wstępne:

- Na komputerze zdalnym jest zainstalowany agent ochrony, który jest zarejestrowany na serwerze zarządzania.
- Komputer ma przypisaną odpowiednią licencję Cyber Protect.
- Na komputerze, z którego jest inicjowane połączenie, jest zainstalowany klient usługi Podłączanie pulpitu zdalnego.
- Komputer, z którego jest inicjowane połączenie RDP, musi mieć dostęp do serwera zarządzania przy użyciu nazwy hosta. Ustawienia DNS muszą być prawidłowo skonfigurowane lub nazwa hosta serwera zarządzania musi się znajdować w pliku hosts.

Połączenie zdalne można nawiązywać zarówno z komputerów z systemem Windows, jak i z komputerów z systemem macOS.



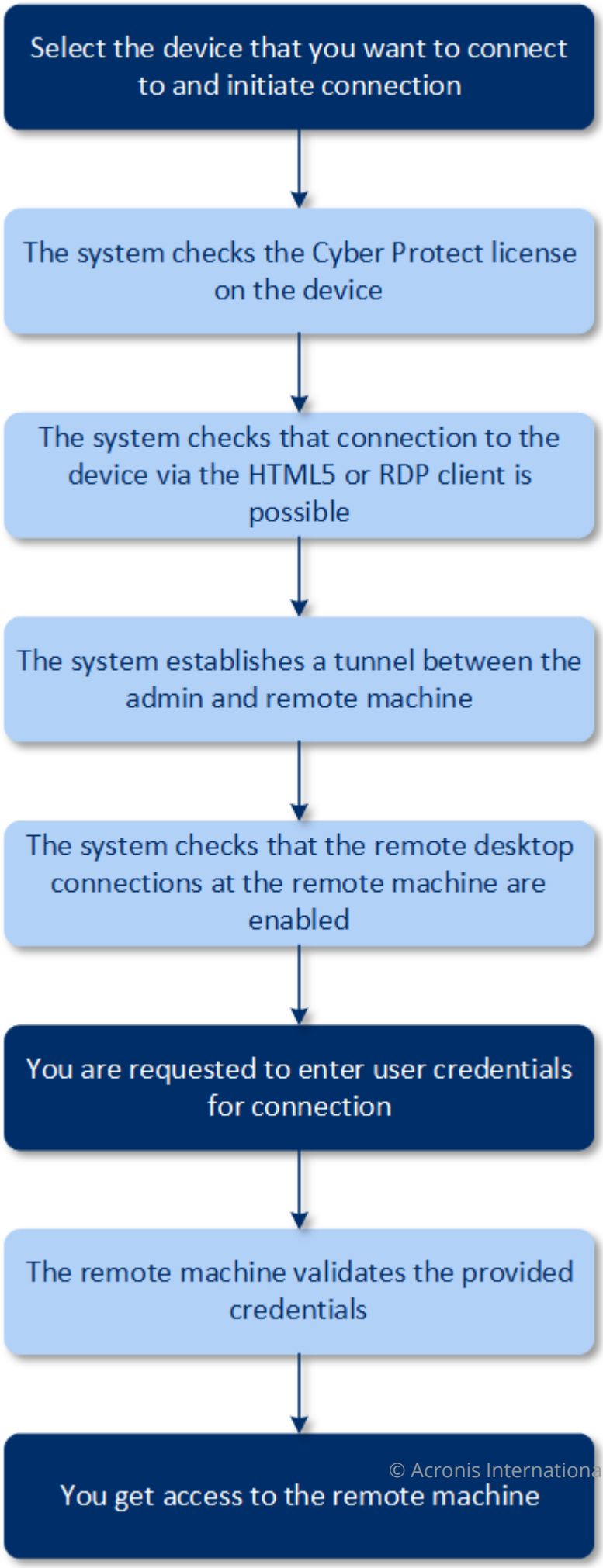
Funkcja dostępu zdalnego może służyć do nawiązywania połączenia z komputerami z systemem Windows z dostępną funkcją pulpitu zdalnego systemu Windows. Dlatego nie można uzyskać dostępu zdalnego na przykład do komputera z systemem Windows 10 Home lub macOS.

Aby nawiązać połączenie z komputerem zdalnym z komputera z systemem macOS, należy dopilnować, aby na komputerze z systemem macOS były zainstalowane następujące aplikacje:

- Klient usługi podłączania pulpitu zdalnego
- Aplikacja Pulpit zdalny Microsoft

Sposób działania

Kiedy próbujesz nawiązać połączenie z komputerem zdalnym, system najpierw sprawdza, czy ten komputer ma licencję produktu Cyber Protect. Następnie sprawdza, czy jest możliwe połączenie przez klienta HTML5 lub RDP. Inicjujesz połączenie za pośrednictwem klienta RDP lub HTML5. System tworzy tunel do komputera zdalnego i sprawdza, czy na tym komputerze są włączone połączenia pulpitu zdalnego. Następnie Ty podajesz poświadczenia, a gdy zostanie sprawdzona ich poprawność, możesz uzyskać dostęp do komputera zdalnego.



Jak nawiązać połączenie z komputerem zdalnym

Aby nawiązać połączenie z komputerem zdalnym:

1. W konsoli internetowej Cyber Protect przejdź do sekcji **Urządzenia** > **Wszystkie urządzenia**.
2. Kliknij komputer, z którym chcesz się połączyć zdalnie, a następnie kliknij **Pulpit cyberochrony** / **Połącz przez klienta RDP** lub **Połącz przez klienta HTML5**.

   Uwaga
   Połączenie przez klienta HTML5 jest dostępne tylko wtedy, gdy serwer zarządzania jest zainstalowany na komputerze z systemem Linux.

3. [Opcjonalnie, tylko w przypadku połączenia przez klienta RDP] Pobierz i zainstaluj klienta usługi Podłączanie pulpitu zdalnego. Zainicjuj połączenie z komputerem zdalnym.
4. Podaj nazwę logowania i hasło w celu uzyskania dostępu komputera, a następnie kliknij **Połącz**.

W wyniku tego uzyskujesz połączenie z komputerem zdalnym i możesz nim zarządzać.

Udostępnianie połączenia zdalnego

Osoby pracujące w domu mogą potrzebować dostępu do swoich biurowych komputerów, podczas gdy firma może nie mieć skonfigurowanej sieci VPN ani innych narzędzi do połączeń zdalnych. Cyber Protect umożliwia udostępnianie połączenia RDP innym użytkownikom, co umożliwia im uzyskiwanie dostępu zdalnego do ich komputerów.

Aby włączyć funkcję udostępniania połączenia zdalnego

1. W konsoli internetowej Cyber Protect przejdź do sekcji **Ustawienia** > **Ochrona** > **Połączenie zdalne**.
2. Zaznacz pole wyboru **Udostępnij połączenie pulpitu zdalnego**.

W wyniku tego po wybraniu urządzenia w konsoli internetowej Cyber Protect pojawi się nowa opcja **Udostępnij połączenie zdalne**.

Aby udostępnić użytkownikom połączenie zdalne

1. W konsoli internetowej Cyber Protect przejdź do sekcji **Urządzenia** > **Wszystkie urządzenia**.
2. Wybierz urządzenie, którego dotyczy udostępniane połączenie zdalne.
3. Kliknij **Udostępnij połączenie zdalne**.
4. Kliknij **Uzyskaj łącze**. W otwartym oknie skopiuj wygenerowane łącze. Możesz je udostępnić użytkownikowi, który potrzebuje zdalnego dostępu do danego urządzenia. Będzie ono działać przez 10 godzin.

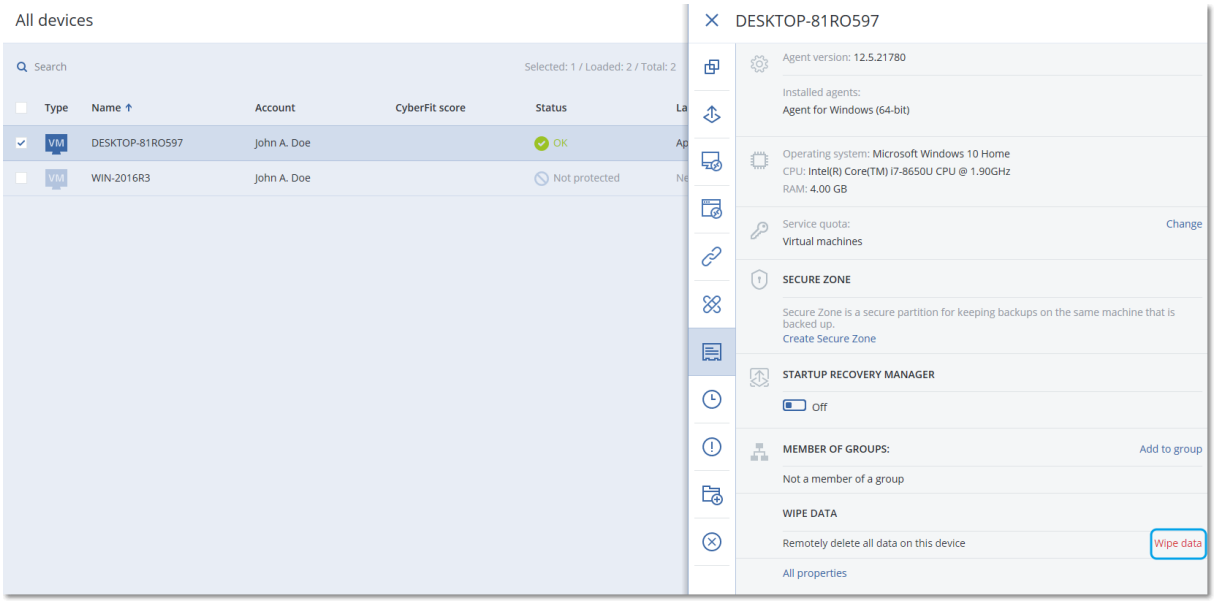
Uzyskane łącze można udostępnić za pośrednictwem poczty e-mail lub innego kanału komunikacji. Użytkownik, któremu zostało udostępnione łącze, musi je kliknąć, a następnie wybrać typ połączenia:

- Połącz przez klienta RDP.
  To połączenie spowoduje pobranie i zainstalowanie klienta połączeń zdalnych.
- Połącz przez klienta HTML5.
  To połączenie nie wymaga instalacji klienta RDP na komputerze użytkownika. Użytkownik zostanie przekierowany do ekranu logowania i musi podać poświadczenia dostępu do komputera.

Wymazywanie zdalne

Funkcja Wymazywanie zdalne umożliwia administratorowi usługi Cyber Protect i właścicielowi komputera usunięcie danych na komputerze zarządzanym, na przykład w przypadku jego zgubienia lub kradzieży. Zapobiegnie to nieuprawnionemu dostępowi do wrażliwych danych.

Wymazywanie zdalne jest dostępne tylko w przypadku komputerów z systemem Windows 10. Aby otrzymać polecenie wymazania, komputer musi być włączony i podłączony do Internetu.



Aby wymazać dane z komputera

1. W konsoli internetowej Cyber Protect przejdź do sekcji **Urządzenia** > **Wszystkie urządzenia**.
2. Wybierz komputer, którego dane chcesz wymazać.

   Uwaga
   Dane można wymazywać tylko z pojedynczych komputerów.

3. Kliknij **Szczegóły**, a następnie kliknij **Wymaż dane**.
   Jeśli wybrany komputer jest w trybie offline, opcja **Wymaż dane** jest niedostępna.
4. Potwierdź wybór.
5. Podaj poświadczenia lokalnego administratora komputera i kliknij **Wymaż dane**.

   Uwaga
   Szczegóły procesu wymazywania i jego inicjatora można sprawdzić w sekcji **Pulpit nawigacyjny** > **Działania**.

Grupy urządzeń

Grupy urządzeń służą do wygodnego zarządzania dużą liczbą zarejestrowanych urządzeń.

Istnieje możliwość zastosowania planu ochrony do grupy. Gdy nowe urządzenie pojawi się w grupie, staje się ono chronione przez plan. Jeśli urządzenie zostanie usunięte z grupy, nie będzie ono już chronione przez plan. Planu zastosowanego do grupy nie można odwołać z elementu grupy, a tylko z samej grupy.

Do grupy można dodać tylko urządzenia tego samego typu. Na przykład w obszarze **Hyper-V** możesz utworzyć maszyny wirtualne Hyper-V. W obszarze **Komputery z agentami** możesz utworzyć grupę komputerów z zainstalowanymi agentami. W obszarze **Wszystkie komputery** nie możesz utworzyć grupy.

Pojedyncze urządzenie może być członkiem więcej niż jednej grupy.

Grupy wbudowane

Gdy urządzenie zostanie zarejestrowane, pojawi się w jednej z wbudowanych grup głównych na karcie **Urządzenia**.

Grup głównych *nie można* edytować ani usuwać. Do grup głównych *nie można* stosować planów.

Niektóre grupy główne zawierają wbudowane grupy podrzędne. Tych grup *nie można* edytować ani usuwać. Jednak do podrzędnych grup wbudowanych *możesz* stosować plany.

Grupy niestandardowe

Ze względu na różne role komputerów ochrona wszystkich urządzeń z wbudowanej grupy za pomocą jednego planu ochrony może nie wystarczyć. Chronione dane każdego działu mają swoją specyfikę. Kopie zapasowe niektórych danych trzeba tworzyć bardzo często, a innych dwa razy do roku. Dobrym rozwiązaniem może być utworzenie różnych planów ochrony dla różnych zestawów komputerów. W takim przypadku warto rozważyć utworzenie grup niestandardowych.

Grupa niestandardowa może zawierać jedną lub więcej grup zagnieżdżonych. Każdą grupę niestandardową można edytować lub usunąć. Istnieją następujące typy grup niestandardowych:

- **Grupy statyczne**

  Grupy statyczne obejmują komputery, które zostały dodane do nich ręcznie. Ich zawartość może zmienić się tylko wtedy, gdy komputer zostanie jawnie dodany lub usunięty.

  Przykład: Tworzysz grupę niestandardową działu księgowości i ręcznie dodajesz do niej komputery księgowych. Komputery księgowych zostaną objęte ochroną po zastosowaniu do tej grupy planu ochrony. Po zatrudnieniu nowej osoby w tym dziale trzeba będzie ręcznie dodać nowy komputer do grupy.
- **Grupy dynamiczne**

Grupy dynamiczne obejmują komputery dodawane automatycznie na podstawie kryteriów wyszukiwania określonych podczas tworzenia grupy. Zawartość grupy dynamicznej zmienia się automatycznie. Komputer należy do grupy dopóty, dopóki spełnia określone kryteria.

Przykład 1: Nazwy hostów komputerów należących do działu księgowości zawierają słowo „księgowość". Możesz podać część nazwy komputera jako kryterium członkostwa w grupie i zastosować do niej plan ochrony. W przypadku zatrudnienia nowego księgowego nowy komputer zostanie dodany do grupy z chwilą rejestracji, a następnie automatycznie objęty ochroną.

Przykład 2: Dział księgowości stanowi odrębną jednostkę organizacyjną (OU) usługi Active Directory. Możesz określić jednostkę organizacyjną Księgowość jako kryterium członkostwa w grupie i zastosować do niej plan ochrony. W przypadku zatrudnienia nowego księgowego nowy komputer zostanie dodany do grupy z chwilą rejestracji i dodania do jednostki organizacyjnej (bez względu na to, co nastąpi pierwsze), a następnie automatycznie objęty ochroną.

Tworzenie grupy statycznej

1. Kliknij **Urządzenia**, a następnie wybierz wbudowaną grupę, która zawiera urządzenia, dla których chcesz utworzyć grupę statyczną.
2. Kliknij ikonę koła zębatego obok grupy, w której chcesz utworzyć grupę.
3. Kliknij **Nowa grupa**.
4. Określ nazwę grupy, a następnie kliknij **OK**.
   W drzewie grup pojawi się nowa grupa.

Dodawanie urządzeń do grup statycznych

1. Kliknij **Urządzenia**, a następnie wybierz urządzenia, które chcesz dodać do grupy.
2. Kliknij **Dodaj do grupy**.
   Oprogramowanie wyświetli drzewo grup, do którego można dodać wybrane urządzenie.
3. Jeśli chcesz utworzyć nową grupę, wykonaj następujące czynności. W przeciwnym razie pomiń ten krok.
   a. Wybierz grupę, w której chcesz utworzyć grupę.
   b. Kliknij **Nowa grupa**.
   c. Określ nazwę grupy, a następnie kliknij **OK**.
4. Wybierz grupę, do której chcesz dodać urządzenie, a następnie kliknij **Gotowe**.

Aby dodać urządzenia do grupy statycznej, możesz też wybrać grupę i kliknąć **Dodaj urządzenia**.

Tworzenie grupy dynamicznej

1. Kliknij **Urządzenia**, a następnie wybierz grupę, która zawiera urządzenia, dla których chcesz utworzyć grupę dynamiczną.

2. Wyszukaj urządzenia przy użyciu pola wyszukiwania. Możesz użyć wielu spośród opisanych niżej atrybutów i operatorów.
3. Kliknij **Zapisz jako** obok pola wyszukiwania.

> **Uwaga**
> W przypadku tworzenia grup niektóre atrybuty nie są obsługiwane. Zobacz tabelę w sekcji „Zapytanie wyszukiwania” poniżej.

4. Określ nazwę grupy, a następnie kliknij **OK**.

Zapytanie wyszukiwania

W poniższej tabeli zestawiono dostępne atrybuty, których można używać w zapytaniach wyszukiwania.

Atrybut	Znaczenie	Przykłady kwerendy wyszukiwania	Obsługiwane w przypadku tworzenia grup
`name`	• Nazwa hosta dla komputerów fizycznych • Nazwa dla maszyn wirtualnych • Nazwa bazy danych • Adres e-mail dla skrzynek pocztowych	`name = 'en-00'`	Tak
`parameters.MacAddress`	Adres MAC.	`parameters.MacAddress LIKE '00-22-4D-50-25-E5'`	Tak
`comment`	Komentarz dotyczący urządzenia. Może on zostać określony automatycznie lub ręcznie. Wartość domyślna: • W przypadku komputerów fizycznych z systemem Windows jest to opis komputera automatycznie skopiowany jako	`comment = 'important machine'` `comment = ''` (wszystkie komputery bez komentarza)	Tak

Atrybut	Znaczenie	Przykłady kwerendy wyszukiwania	Obsługiwane w przypadku tworzenia grup

	komentarz. Ta wartość jest synchronizowana co 15 minut.
	• W przypadku innych urządzeń pozostaje pusty.
	
	Uwaga
	Jeśli ręcznie dodasz tekst w polu komentarza, automatyczna synchronizacja opisu w systemie Windows zostanie wyłączona. Aby ją ponownie włączyć, usuń dodany komentarz.
	
	Aby odświeżyć automatycznie synchronizowane komentarze dotyczące swoich urządzeń, ponownie uruchom usługę komputera zarządzanego w sekcji **Usługi systemu Windows** lub uruchom w wierszu polecenia następujące polecenia:
	`net stop mms`
	`net start mms`
	Aby wyświetlić komentarz, wybierz urządzenie w obszarze **Urządzenia**, kliknij **Szczegóły**, a następnie		

Atrybut	Znaczenie	Przykłady kwerendy wyszukiwania	Obsługiwane w przypadku tworzenia grup
	znajdź sekcję **Komentarz**. Aby dodać lub zmienić komentarz, kliknij **Dodaj** lub **Edytuj**. W przypadku urządzeń, na których jest zainstalowany agent ochrony, istnieją dwa osobne pola komentarzy: • Komentarz dotyczący agenta ◦ W przypadku komputerów fizycznych z systemem Windows jest to opis komputera automatycznie skopiowany jako komentarz. Ta wartość jest synchronizowana co 15 minut. ◦ W przypadku innych urządzeń pozostaje pusty. **Uwaga** Jeśli ręcznie dodasz tekst w polu komentarza, automatyczna synchronizacja opisu w systemie Windows zostanie wyłączona. Aby ją ponownie włączyć, usuń dodany komentarz.		

Atrybut	Znaczenie	Przykłady kwerendy wyszukiwania	Obsługiwane w przypadku tworzenia grup
	• Komentarz dotyczący urządzenia ◦ Jeśli komentarz dotyczący agenta zostanie dodany automatycznie, zostanie on skopiowany jako komentarz dotyczący urządzenia. Ręcznie dodane komentarze dotyczące agenta nie są kopiowane jako komentarze dotyczące urządzenia. ◦ Komentarze dotyczące urządzenia nie są kopiowane jako komentarze dotyczące agenta. W przypadku urządzenia może zostać dodany co najmniej jeden z tych dwóch komentarzy. Mogą one też pozostać puste. W przypadku dodania obu tych komentarzy komentarz dotyczący urządzenia ma pierwszeństwo. Aby wyświetlić komentarz dotyczący agenta, w obszarze **Ustawienia** > **Agenci** wybierz urządzenie z agentem, kliknij **Szczegóły**, a następnie		

Atrybut	Znaczenie	Przykłady kwerendy wyszukiwania	Obsługiwane w przypadku tworzenia grup
	znajdź sekcję **Komentarz**. Aby wyświetlić komentarz dotyczący urządzenia, wybierz je w obszarze **Urządzenia**, kliknij **Szczegóły**, a następnie znajdź sekcję **Komentarz**. Aby ręcznie dodać lub zmienić komentarz, kliknij **Dodaj** lub **Edytuj**.		
`ip`	Adres IP (tylko w przypadku komputerów fizycznych).	`ip RANGE ('10.250.176.1','10.250.176.50')`	Tak
`cpuArch`	Architektura CPU. Możliwe wartości: • `'x64'` • `'x86'`	`cpuArch = 'x64'`	Tak
`memorySize`	Rozmiar pamięci RAM w megabajtach (MB).	`memorySize < 1024`	Tak
`cpuName`	Nazwa procesora.	`cpuName LIKE '%XEON%'`	Tak
`insideVm`	Maszyna wirtualna zawierająca agenta. Możliwe wartości: • `true` • `false`	`insideVm = true`	Tak
`tzOffset`	Przesunięcie strefy czasowej komputera w minutach.	`tzOffset = 120`	Tak
`parameters.Architecture`	Architektura systemu operacyjnego. Możliwe wartości: • `'x86'`	`parameters.Architecture = 'x86'`	Tak

Atrybut	Znaczenie	Przykłady kwerendy wyszukiwania	Obsługiwane w przypadku tworzenia grup
	• `'x64'`		
`osName`	Nazwa systemu operacyjnego.	`osName LIKE '%Windows XP%'`	Tak
`osType`	Typ systemu operacyjnego. Możliwe wartości: • `'windows'` • `'linux'` • `'macosx'`	`osType IN ('linux', 'macosx')`	Tak
`osProductType`	Typ produktu systemu operacyjnego. Możliwe wartości: • `'dc'` Oznacza kontroler domeny. • `'server'` • `'workstation'`	`osProductType = 'server'`	Tak
`virtualType`	Typ maszyny wirtualnej. Możliwe wartości: • `'vmwesx'` Maszyny wirtualne VMware. • `'mshyperv'` Maszyny wirtualne Hyper-V. • `'pcs'` Maszyny wirtualne Virtuozzo. • `'hci'` Maszyny wirtualne Virtuozzo Hybrid Infrastructure. • `'scale'` Maszyny wirtualne Scale Computing	`virtualType = 'vmwesx'`	Tak

Atrybut	Znaczenie	Przykłady kwerendy wyszukiwania	Obsługiwane w przypadku tworzenia grup
	HC3. • `'ovirt'` Maszyny wirtualne oVirt		
`osSp`	Dodatek Service Pack systemu operacyjnego.	`osSp = 1`	Tak
`osVersionMajor`	Wersja główna systemu operacyjnego.	`osVersionMajor = 1`	Tak
`osVersionMinor`	Wersja poprawkowa systemu operacyjnego.	`osVersionMminor = 1`	Tak
`isOnline`	Dostępność komputera. Możliwe wartości: • `true` • `false`	`isOnline = true`	Nie
`tenant`	Nazwa jednostki, do której należy urządzenie.	`tenant = 'Unit 1'`	Tak
`tenantId`	Identyfikator jednostki, do której należy urządzenie. Aby uzyskać identyfikator jednostki, w obszarze **Urządzenia** wybierz urządzenie, kliknij **Szczegóły** > **Wszystkie właściwości**. Identyfikator jest pokazywany w polu `ownerId`.	`tenantId = '3bfe6ca9-9c6a-4953-9cb2-a1323f454fc9'`	Tak
`state`	Stan urządzenia. Możliwe wartości: • `'idle'` • `'interactionRequired'` • `'canceling'`	`state = 'backup'`	Nie

Atrybut	Znaczenie	Przykłady kwerendy wyszukiwania	Obsługiwane w przypadku tworzenia grup
	• `'backup'` • `'recover'` • `'install'` • `'reboot'` • `'failback'` • `'testReplica'` • `'run_from_image'` • `'finalize'` • `'failover'` • `'replicate'` • `'createAsz'` • `'deleteAsz'` • `'resizeAsz'`		
`status`	Stan zasobów. Możliwe wartości: • `'notProtected'` • `'ok'` • `'warning'` • `'error'` • `'critical'`	`status = 'ok'`	Nie
`protectedByPlan`	Urządzenia, które są chronione przez plan ochrony o danym identyfikatorze. Aby uzyskać identyfikator planu, kliknij **Plany** > **Kopia zapasowa**, wybierz plan, kliknij diagram w kolumnie **Status**, a następnie kliknij status. Zostanie utworzone nowe wyszukiwanie z identyfikatorem planu.	`protectedByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'`	Nie
`okByPlan`	Urządzenia, które są chronione przez plan ochrony o danym	`okByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'`	Nie

Atrybut	Znaczenie	Przykłady kwerendy wyszukiwania	Obsługiwane w przypadku tworzenia grup
	identyfikatorze i mają status **OK**.		
`errorByPlan`	Urządzenia, które są chronione przez plan ochrony o danym identyfikatorze i mają status **Błąd**.	`errorByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'`	Nie
`warningByPlan`	Urządzenia, które są chronione przez plan ochrony o danym identyfikatorze i mają status **Ostrzeżenie**.	`warningByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'`	Nie
`runningByPlan`	Urządzenia, które są chronione przez plan ochrony o danym identyfikatorze i mają status **Uruchomione**.	`runningByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'`	Nie
`interactionByPlan`	Urządzenia, które są chronione przez plan ochrony o danym identyfikatorze i mają status **Wymagane działanie**.	`interactionByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'`	Nie
`ou`	Komputery należące do wskazanej jednostki organizacyjnej w usłudze Active Directory.	`ou IN ('RnD', 'Computers')`	Tak
`id`	Identyfikator urządzenia. Aby uzyskać identyfikator urządzenia, w obszarze **Urządzenia** wybierz urządzenie, kliknij **Szczegóły** > **Wszystkie właściwości**. Identyfikator jest pokazywany w polu `id`.	`id != '4B2A7A93-A44F-4155-BDE3-A023C57C9431'`	Tak

Atrybut	Znaczenie	Przykłady kwerendy wyszukiwania	Obsługiwane w przypadku tworzenia grup

`lastBackupTime`	Data i godzina ostatniego pomyślnego utworzenia kopii zapasowej.
	Format jest następujący: `'RRRR-MM-DD GG:MM'`.
		`lastBackupTime > '2022-03-11'`
		`lastBackupTime <= '2022-03-11 00:15'`
		`lastBackupTime is null`
			Nie

`lastBackupTryTime`	Godzina ostatniej próby utworzenia kopii zapasowej. Format jest następujący: `'RRRR-MM-DD GG:MM'`.	`lastBackupTryTime >= '2022-03-11'`	Nie
`nextBackupTime`	Godzina następnego utworzenia kopii zapasowej. Format jest następujący: `'RRRR-MM-DD GG:MM'`.	`nextBackupTime >= '2022-08-11'`	Nie
`agentVersion`	Wersja zainstalowanego agenta ochrony.	`agentVersion LIKE '12.0.*'`	Tak
`hostId`	Wewnętrzny identyfikator agenta ochrony. Aby uzyskać identyfikator agenta ochrony, w obszarze **Urządzenia** wybierz komputer, kliknij **Szczegóły** > **Wszystkie właściwości**. Użyj wartości „`id`” właściwości `agent`.	`hostId = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'`	Tak
`resourceType`	Typ zasobu. Możliwe wartości: • `'machine'` • `'virtual_machine.vmwesx'` • `'virtual_`	`resourceType = 'machine'` `resourceType in ('mssql_aag_database', 'mssql_database')`	Tak

Atrybut	Znaczenie	Przykłady kwerendy wyszukiwania	Obsługiwane w przypadku tworzenia grup
	`machine.mshyperv'` • `'virtual_machine.rhev'` • `'virtual_machine.kvm'` • `'virtual_machine.xen'`		
`hasAsz`	Agent ochrony na komputerze fizycznym z partycją Acronis Secure Zone. Możliwe wartości: • `true` • `false`	`hasAsz=true`	Tak
`chassis`	Typ komputera. Możliwe wartości: • `unknown` • `laptop` • `desktop` • `server` • `other`	`chassis='laptop'`	Tak

Uwaga
W przypadku pominięcia wartości godziny i minut za czas rozpoczęcia uznaje się RRRRR-MM-DD 00:00, a za czas zakończenia — RRRR-MM-DD 23:59:59. Na przykład lastBackupTime = 2020-02-20 oznacza, że w wynikach wyszukiwania zostaną uwzględnione wszelkie kopie zapasowe utworzone między
lastBackupTime >= 2020-02-20 00:00 a lastBackup time <= 2020-02-20 23:59:59

Operatory

W poniższej tabeli zestawiono dostępne operatory.

Operator	Znaczenie	Przykłady
`AND`	Operator iloczynu logicznego.	`name like 'en-00' AND tenant = 'Unit 1'`

Operator	Znaczenie	Przykłady
`OR`	Operator sumy logicznej.	`state = 'backup' OR state = 'interactionRequired'`
`IN (<value1>,... <valueN>)`	Ten operator służy do sprawdzania, czy wyrażenie jest zgodne z jakąkolwiek wartością na liście wartości.	`osType IN ('windows', 'linux')`
`NOT`	Operator negacji logicznej.	`NOT(osProductType = 'workstation')`
`NOT IN (<value1>,... <valueN>)`	Ten operator jest przeciwieństwem operatora `W`.	`NOT osType IN ('windows', 'linux')`

`LIKE 'wzorzec z symbolem wieloznacznym'`	Ten operator służy do sprawdzania, czy wyrażenie jest zgodne z jakąkolwiek wartością zgodną z określonymi symbolami wieloznacznymi.
	Można użyć następujących operatorów symboli wieloznacznych:
	• * lub % Gwiazdka i znak procentu reprezentują zero, jeden lub wiele znaków
	• _ Podkreślenie reprezentuje pojedynczy znak
		`name LIKE 'en-00'`
		`name LIKE '*en-00'`
		`name LIKE '*en-00*'`
		`name LIKE 'en-00_'`

`RANGE(<starting_value>, <ending_value>)`	Ten operator służy do sprawdzania, czy wyrażenie mieści się w zakresie wartości (włącznie).	`ip RANGE ('10.250.176.1','10.250.176.50')`
`= or ==`	Operator *Równe*.	`osProductType = 'server'`
`!=` lub `<>`	Operator *Różne od*.	`id != '4B2A7A93-A44F-4155-BDE3-A023C57C9431'`
`<`	Operator *Mniej niż*.	`memorySize < 1024`
`>`	Operator *Więcej niż*.	`diskSize > 300GB`
`<=`	Operator *Mniej niż lub równe*.	`lastBackupTime <= '2022-05-11 00:15'`
`>=`	Operator *Więcej niż lub równe*.	`nextBackupTime >= '2022-09-11'`

Stosowanie planu ochrony do grupy

1. Kliknij **Urządzenia**, a następnie wybierz wbudowaną grupę zawierającą grupę, do której chcesz zastosować plan ochrony.

   Oprogramowanie wyświetli listę grup podrzędnych.

2. Wybierz grupę, do której chcesz zastosować plan ochrony.
3. Kliknij **Kopia zapasowa grupy**.

   W oprogramowaniu zostanie wyświetlona lista planów ochrony, które można zastosować do grupy.
4. Wykonaj jedną z następujących czynności:
   - Rozwiń jeden z planów ochrony i kliknij **Zastosuj**.
   - Kliknij **Utwórz nowy** i utwórz nowy plan ochrony zgodnie z opisem podanym w sekcji „Kopia zapasowa”.

Monitorowanie i raportowanie

Pulpit nawigacyjny **Przegląd** umożliwia monitorowanie bieżącego stanu chronionej infrastruktury.

Sekcja **Raporty** umożliwia generowanie, na żądanie lub zgodnie z harmonogramem, raportów dotyczących chronionej infrastruktury. Ta sekcja jest dostępna tylko w przypadku licencji Advanced.

Pulpit nawigacyjny Przegląd

Pulpit nawigacyjny **Przegląd** udostępnia szereg umożliwiających dostosowanie widżetów oferujących ogólny obraz chronionej infrastruktury. Możesz wybierać spośród ponad 20 widżetów prezentowanych jako wykresy kołowe, tabele, wykresy, wykresy słupkowe i listy Mają elementy umożliwiające klikanie, które pozwalają badać i rozwiązywać problemy. Informacje w widżetach są aktualizowane co 5 minut.

Jeśli masz licencję Advanced, możesz też pobrać bieżący stan pulpitu nawigacyjnego lub przesłać go za pomocą poczty e-mail w formacie .pdf oraz/lub .xlsx. Aby wysłać pulpit nawigacyjny przy użyciu poczty e-mail, upewnij się, że są skonfigurowane ustawienia **serwera poczty e-mail**.

Dostępne widżety zależą od wersji programu Cyber Protect. Widżety domyślne wymieniono poniżej:

Widżet	Dostępność	Opis
Cyberochrona	Niedostępny w wersjach Cyber Backup	Przedstawia ogólne informacje o rozmiarze kopii zapasowych, zablokowanym złośliwym oprogramowaniu, zablokowanych adresach URL, znalezionych lukach w zabezpieczeniach i zainstalowanych poprawkach.
Status ochrony	Dostępny we wszystkich wersjach	Przedstawia aktualne statusy ochrony wszystkich komputerów.
Działania	Dostępny we wszystkich wersjach	Umożliwia wyświetlenie podsumowania działań dotyczących taśm, które zostały wykonane we wskazanym okresie.
Podsumowanie aktywnych alertów	Dostępny we wszystkich wersjach	Umożliwia wyświetlenie podsumowania aktywnych alertów według typu i wagi.
Status instalacji poprawek	Niedostępny w wersjach Cyber Backup	Umożliwia wyświetlenie liczby komputerów pogrupowanych według statusu instalacji poprawek.
Brakujące aktualizacje według kategorii	Niedostępny w wersjach Cyber Backup	Umożliwia wyświetlenie liczby brakujących aktualizacji według kategorii.
Status kondycji dysków	Niedostępny w wersjach	Umożliwia wyświetlenie liczby dysków według ich statusów.

	Cyber Backup	
Urządzenia	Dostępny we wszystkich wersjach	Umożliwia wyświetlenie szczegółowych informacji o urządzeniach w danym środowisku.
Szczegóły aktywnych alertów	Dostępny we wszystkich wersjach	Umożliwia wyświetlenie szczegółowych informacji o aktywnych alertach.
Występujące luki w zabezpieczeniach	Dostępny we wszystkich wersjach	Przedstawia istniejące luki w zabezpieczeniach systemów operacyjnych i aplikacji w Twoim środowisku oraz komputery, których te problemy dotyczą.
Historia instalacji poprawek	Niedostępny w wersjach Cyber Backup	Umożliwia wyświetlenie szczegółowych informacji o zainstalowanych poprawkach.
Ostatnie objęte wpływem	Dostępny we wszystkich wersjach	Umożliwia wyświetlenie szczegółowych informacji o ostatnio zainfekowanych komputerach.
Podsumowanie lokalizacji	Dostępny we wszystkich wersjach	Umożliwia wyświetlenie szczegółowych informacji o lokalizacjach kopii zapasowych.

Aby dodać widżet

Kliknij **Dodaj widżet** i wykonaj jedną z następujących czynności:

- Kliknij widżet, który chcesz dodać. Widżet zostanie dodany z domyślnymi ustawieniami.
- Aby edytować widżet przed dodaniem, zaznacz go i kliknij ikonę ołówka. Po skończonej edycji widżetu kliknij **Gotowe**.

Aby zmienić ustawienie widżetów na pulpicie nawigacyjnym

Widżety można przeciągać, klikając ich nazwy.

Aby edytować widżet

Kliknij ikonę ołówka obok nazwy widżetu. Edycja widżetu pozwala zmienić jego nazwę, zmodyfikować zakres czasu, ustawić filtry i pogrupować wiersze.

Aby usunąć widżet

Kliknij symbol X obok nazwy widżetu.

Cyber Protection

Ten widżet przedstawia ogólne informacje o rozmiarze kopii zapasowych, zablokowanym złośliwym oprogramowaniu, zablokowanych adresach URL, znalezionych lukach w zabezpieczeniach i zainstalowanych poprawkach.

W górnym wierszu znajdują się bieżące dane statystyczne:

- **Uwzględnione w kopii zapasowej dzisiaj** — suma rozmiarów punktów odzyskiwania z ostatnich 24 godzin
- **Zablokowane złośliwe oprogramowanie** — liczba obecnie aktywnych alertów dotyczących zablokowanego złośliwego oprogramowania
- **Zablokowane adresy URL** — liczba obecnie aktywnych alertów dotyczących zablokowanych adresów URL
- **Występujące luki w zabezpieczeniach** — liczba obecnie występujących luk w zabezpieczeniach
- **Poprawki gotowe do instalacji** — liczba aktualnie dostępnych poprawek do zainstalowania

W dolnym wierszu znajdują się statystyki ogólne:

- Rozmiar wszystkich kopii zapasowych po kompresji
- Łączna liczba zablokowanych złośliwych programów na wszystkich komputerach
- Łączna liczba zablokowanych adresów URL na wszystkich komputerach
- Łączna liczba wykrytych luk w zabezpieczeniach na wszystkich komputerach
- Łączna liczba zainstalowanych aktualizacji/poprawek na wszystkich komputerach

Status ochrony

Status ochrony

Ten widżet umożliwia wyświetlenie aktualnego statusu ochrony wszystkich komputerów.

Komputer może mieć jeden z następujących statusów:

- **Chronione** — komputery z zastosowanym planem ochrony.
- **Niechronione** — komputery bez zastosowanego planu ochrony. Są to zarówno wykryte, jak i zarządzane komputery, do których nie zastosowano planu ochrony.
- **Zarządzane** — komputery z zainstalowanym agentem ochrony.
- **Wykryto** — komputery bez zainstalowanego agenta ochrony.

Kliknięcie statusu komputera spowoduje przejście do listy komputerów o danym statusie, gdzie można znaleźć dodatkowe informacje.

Wykryte komputery

Ten widżet przedstawia listę komputerów wykrytych we wskazanym okresie.

Monitorowanie kondycji dysków

Monitorowanie kondycji dysków dostarcza informacji o bieżącej kondycji dysku i prognozach na jej temat, dzięki czemu można zapobiec utracie danych, do której mogłoby dojść wskutek awarii dysku. Obsługiwane są zarówno dyski HDD, jak i dyski SSD.

Ograniczenia:

- Prognoza kondycji dysków jest obsługiwana tylko w przypadku komputerów z systemem Windows.
- Monitorowane są tylko dyski komputerów fizycznych. Dyski maszyn wirtualnych nie mogą być monitorowane ani pokazywane na widżetach kondycji dysków.
- Konfiguracje macierzy RAID nie są obsługiwane.
- W przypadku dysków NVMe monitorowanie kondycji dysków jest obsługiwane tylko w przypadku dysków, które przekazują dane SMART za pośrednictwem interfejsu API systemu Windows. Monitorowanie kondycji dysków nie jest obsługiwane w przypadku dysków NVMe, które wymagają odczytu danych SMART bezpośrednio z dysku.

Kondycja dysku może być odzwierciedlana przez jeden z następujących statusów:

- **OK**
  Kondycja dysku w zakresie 70–100%.
- **Ostrzeżenie**
  Kondycja dysku w zakresie 30–70%.
- **Krytyczne**
  Kondycja dysku w zakresie 0–30%.
- **Obliczanie danych dysku**
  Trwa obliczanie aktualnego stanu dysku i generowanie prognozy

Sposób działania

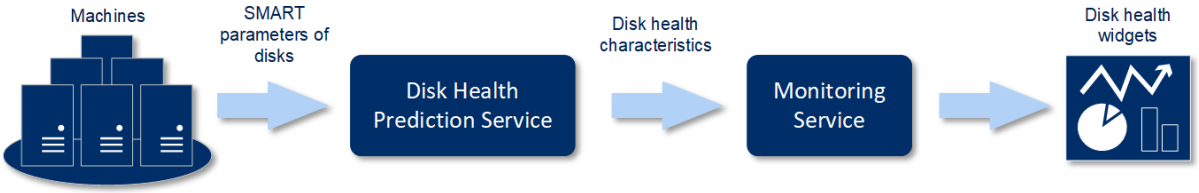
Usługa Prognoza kondycji dysków korzysta z modelu predykcyjnego opartego na sztucznej inteligencji.

1. Agent ochrony zbiera parametry SMART dysków i przekazuje te dane do usługi Prognoza kondycji dysków:
   - SMART 5 — liczba ponownie alokowanych sektorów.
   - SMART 9 — liczba godzin w stanie zasilania.
   - SMART 187 — zgłoszone nienaprawialne błędy.
   - SMART 188 — przekroczony limit czasu wykonywania polecenia.
   - SMART 197 — liczba oczekujących sektorów.
   - SMART 198 — liczba nienaprawialnych sektorów w trybie offline.
   - SMART 200 — wskaźnik błędów zapisu.
2. Usługa Prognoza kondycji dysków przetwarza uzyskane parametry SMART, sporządza prognozy i udostępnia następujące charakterystyki kondycji dysku:
   - Bieżący stan dysku: OK, Ostrzeżenie, Krytyczne.
   - Prognoza kondycji dysków: negatywna, stabilna, pozytywna.

- Prawdopodobieństwo prognozy kondycji dysku w procentach.

Prognoza zawsze dotyczy najbliższego miesiąca.

3. Usługa monitorowania odbiera te właściwości, a następnie wyświetla odpowiednie informacje na widżetach kondycji dysków w konsoli internetowej Cyber Protect.



Widżety kondycji dysków

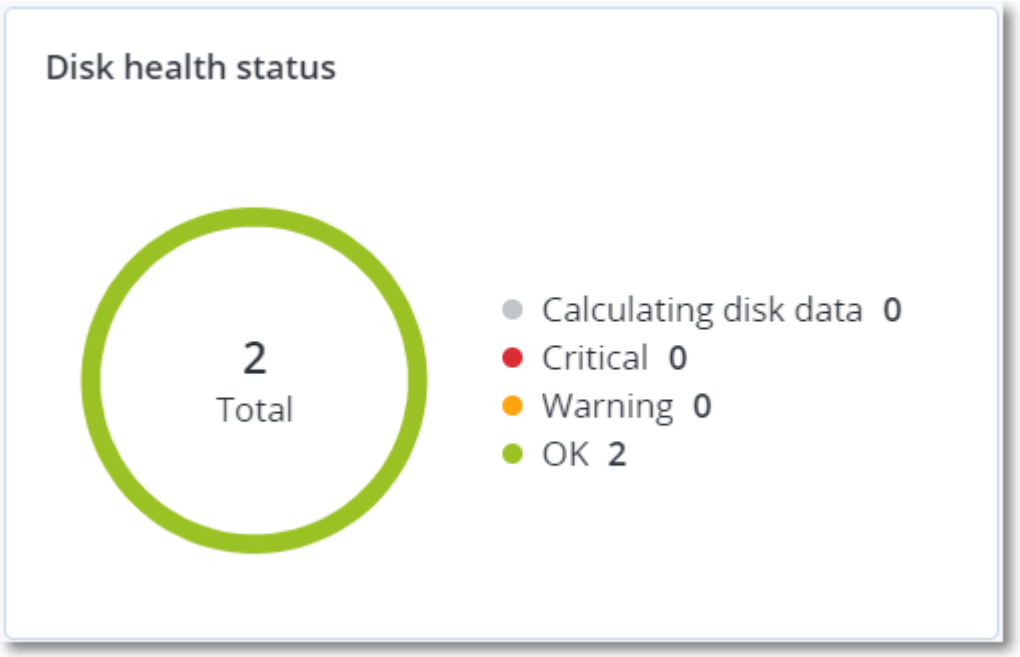
Wyniki monitorowania kondycji dysków są prezentowane na następujących widżetach dostępnych w konsoli internetowej Cyber Protect.

- **Przegląd kondycji dysków** — widżet w formie mapy drzewa obejmującej dwa poziomy szczegółów, które można zmieniać przez pogłębianie analizy.
  - Poziom komputera
    Umożliwia wyświetlenie podsumowania statusów dysków wszystkich komputerów w wybranej jednostce organizacyjnej. Widoczny jest tylko najbardziej krytyczny status dysku. Pozostałe statusy są pokazywane na etykietce wyświetlanej po wskazaniu danego bloku myszą. Rozmiar bloku komputera zależy od łącznego rozmiaru dysków tego komputera. Kolor bloku komputera zależy od najbardziej krytycznego wykrytego statusu dysku.

- Poziom dysku
  Zawiera aktualne statusy kondycji wszystkich dysków wybranego komputera. Każdy blok dysków zawiera jedną z następujących prognoz kondycji dysków wraz z jej prawdopodobieństwem wyrażonym w procentach:
  - Ulegnie pogorszeniu
  - Pozostanie stabilne

- Ulegnie poprawie

- **Status kondycji dysków** — widżet w postaci wykresu kołowego przedstawiający liczby dysków według poszczególnych statusów.



Alerty dotyczące statusów kondycji dysków

Kondycja dysku jest sprawdzana co 30 minut, a raz dziennie jest generowany odpowiedni alert. Gdy stan kondycji dysku zmieni się z **Ostrzeżenie** na **Krytyczne**, zawsze zostanie wygenerowany alert.

Nazwa alertu	Ważność	Status kondycji dysków	Opis
Możliwość awarii dysku	Ostrzeżenie	(30 – 70)	Dysk <nazwa dysku> komputera prawdopodobnie ulegnie awarii. Jak najszybciej utwórz pełną kopię zapasową obrazu dysku, wymień go, a następnie odzyskaj obraz na nowy dysk.
Bliska awaria dysku	Krytyczny	(0 – 30)	Dysk <nazwa dysku> komputera jest w stanie krytycznym i najprawdopodobniej bardzo szybko ulegnie awarii. Nie zaleca się utworzenia kopii zapasowej obrazu tego dysku, ponieważ dodatkowe obciążenie może spowodować jego awarię. Niezwłocznie utwórz kopię zapasową wszystkich najważniejszych plików z tego dysku i go wymień.

Mapa ochrony danych

Funkcja mapy ochrony danych pozwala na wykrycie wszystkich ważnych danych i uzyskanie szczegółowych informacji o liczbie, rozmiarze, lokalizacji, statusach ochrony wszystkich ważnych plików w skalowalnym widoku mapy drzewa.

Rozmiar każdego bloku zależy od łącznej liczby lub łącznego rozmiaru wszystkich ważnych plików danej jednostki organizacyjnej lub komputera.

Pliki mogą mieć jeden z następujących statusów ochrony:

- **Krytyczny** — 51–100% niechronionych plików z podanymi rozszerzeniami, które nie są uwzględniane w kopiach zapasowych i nie będą uwzględniane w kopiach zapasowych przy obecnych ustawieniach tworzenia kopii zapasowych wybranego komputera lub wybranej lokalizacji.
- **Niski** — 21–50% niechronionych plików z podanymi rozszerzeniami, czyli plików, które nie są uwzględniane w kopiach zapasowych i nie będą uwzględniane w kopiach zapasowych przy obecnych ustawieniach tworzenia kopii zapasowych wybranego komputera lub wybranej lokalizacji.
- **Średni** — 1–20% niechronionych plików z podanymi rozszerzeniami, czyli plików, które nie są uwzględniane w kopiach zapasowych i nie będą uwzględniane w kopiach zapasowych przy obecnych ustawieniach tworzenia kopii zapasowych wybranego komputera lub wybranej lokalizacji.

- **Wysoki** — wszystkie pliki z podanymi rozszerzeniami są chronione (uwzględniane w kopiach zapasowych) w przypadku wybranego komputera lub wybranej lokalizacji.

Wyniki kontroli ochrony danych można znaleźć na pulpicie nawigacyjnym w widżecie Mapa ochrony danych — jest to mapa drzewa ze szczegółowymi informacjami na poziomie komputera.

Zatrzymaj wskaźnik myszy na kolorowym bloku, aby wyświetlić dodatkowe informacje o liczbie niechronionych plików i ich lokalizacjach. Aby objąć te pliki ochroną, kliknij **Chroń wszystkie pliki**.

Widżety dotyczące oceny luk w zabezpieczeniach

Komputery z lukami w zabezpieczeniach

Ten widżet przedstawia komputery z lukami w zabezpieczeniach uporządkowane według ważności luk.

Znaleziona luka może mieć jeden z następujących poziomów ważności określony zgodnie z systemem Common Vulnerability Scoring System (CVSS) w wersji 3.0:

- Bezpieczny: nie znaleziono luk w zabezpieczeniach
- Krytyczny: 9,0–10,0 w skali CVSS
- Wysoki: 7,0–8,9 w skali CVSS
- Średni: 4,0–6,9 w skali CVSS
- Niski: 0,1–3,9 w skali CVSS
- Brak: 0,0 w skali CVSS

Występujące luki w zabezpieczeniach

Ten widżet przedstawia obecnie występujące luki w zabezpieczeniach na komputerach. W widżecie **Istniejące luki w zabezpieczeniach** są dostępne dwie kolumny z sygnaturami czasowymi:

- **Pierwsze wykrycie** — data i godzina pierwszego wykrycia luki na komputerze.
- **Ostatnie wykrycie** — data i godzina ostatniego wykrycia luki na komputerze.

Widżety dotyczące instalacji poprawek

Występują cztery widżety związane z funkcjami zarządzania poprawkami.

Status instalacji poprawek

Ten widżet przedstawia liczbę komputerów pogrupowanych według statusów instalacji poprawek.

- **Zainstalowane** — na komputerze zainstalowano wszystkie dostępne poprawki
- **Wymagane ponowne uruchomienie** — po zainstalowaniu poprawki wymagane jest ponowne uruchomienie komputera
- **Niepowodzenie** — instalacja poprawki zakończyła się niepowodzeniem

Podsumowanie instalacji poprawek

Ten widżet przedstawia podsumowanie poprawek według statusów ich instalacji.

Historia instalacji poprawek

Ten widżet umożliwia wyświetlenie szczegółowych informacji o poprawkach zainstalowanych na komputerach.

Brakujące aktualizacje według kategorii

Ten widżet przedstawia liczbę brakujących aktualizacji według kategorii. Pokazywane są następujące kategorie:

- Aktualizacje zabezpieczeń
- Aktualizacje krytyczne
- Inne

Szczegóły skanowania kopii zapasowej

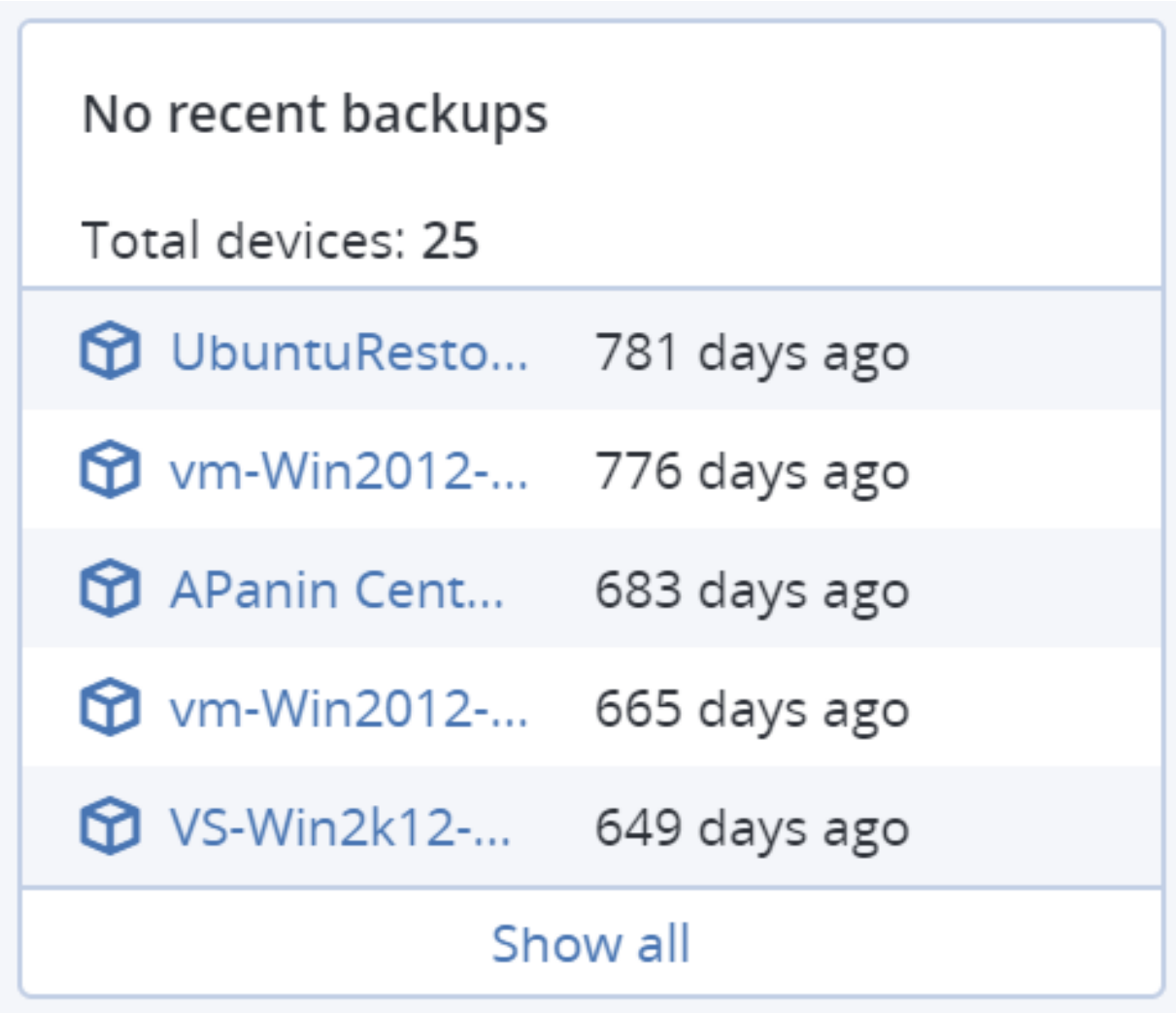
Ten widżet jest dostępny tylko wtedy, gdy na serwerze zarządzania jest zainstalowana usługa Skanowanie. Umożliwia wyświetlenie szczegółowych informacji o zagrożeniach wykrytych w kopiach zapasowych.

Ostatnie objęte wpływem

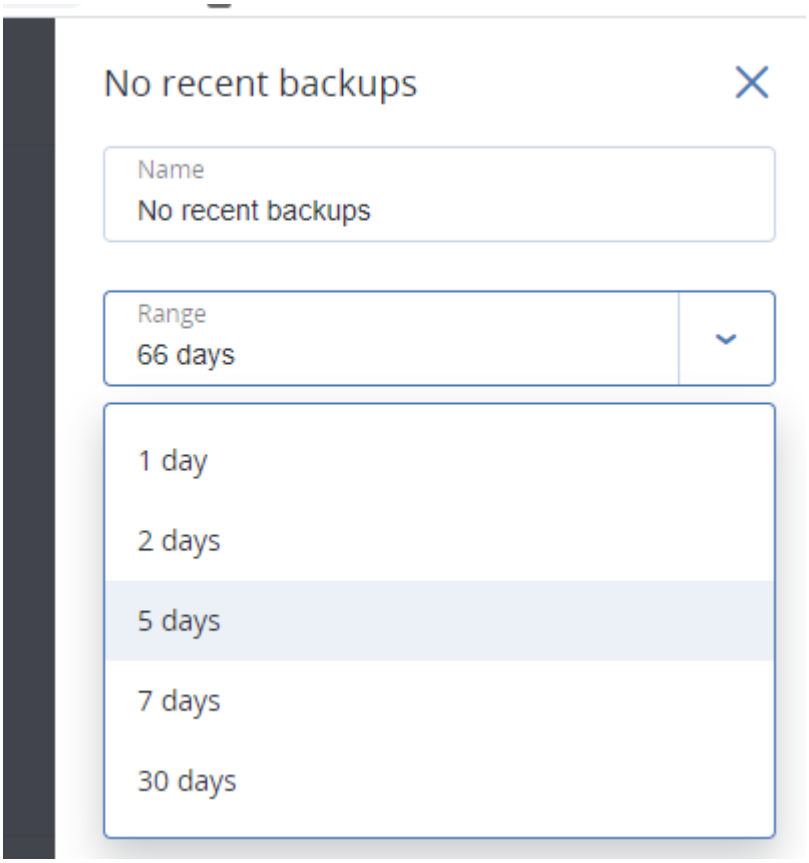
Ten widżet umożliwia wyświetlenie szczegółowych informacji o ostatnio zainfekowanych komputerach. Można tu sprawdzić, jakie wykryto zagrożenie i ile plików zostało zainfekowanych.

Brak ostatnich kopii zapasowych

Ten widżet przedstawia obciążenia z zastosowanymi planami ochrony, w których przypadku data ostatniej udanej kopii zapasowej jest wcześniejsza niż okres zdefiniowany w ustawieniach widżetu.



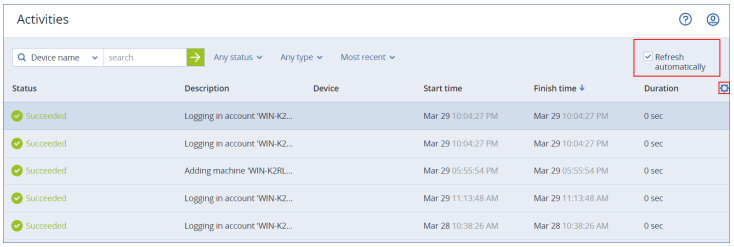
W razie dodania tego widżetu domyślnie zawiera on informacje z ostatnich 5 dni. Można wybrać inny okres za pomocą menu rozwijanego lub ręcznie wprowadzić liczbę dni. Można wprowadzić maksymalnie 180 dni.



Karta Działania

Karta **Działania** zawiera przegląd działań z ostatnich 90 dni.

Aby dostosować widok na karcie **Działania**, kliknij ikonę koła zębatego i wybierz kolumny do wyświetlenia. Aby móc sprawdzać postęp działań w czasie rzeczywistym, zaznacz pole wyboru **Odświeżaj automatycznie**. Pamiętaj, że częste aktualizowanie wielu działań może obniżyć wydajność serwera zarządzania.



Listę działań można przeszukiwać według następujących kryteriów:

- **Nazwa urządzenia**
  Jest to komputer, na którym jest wykonywane dane działanie.
- **Rozpoczęte przez**
  To jest konto, z którego rozpoczęto dane działanie.

Działania można też filtrować według następujących właściwości:

- **Status**
  Na przykład wykonane pomyślnie, niepowodzenie, w toku lub anulowane.
- **Typ**
  Na przykład stosowanie planu, usuwanie kopii zapasowych czy instalowanie aktualizacji oprogramowania.
- **Czas**
  Na przykład ostatnie działania, działania z ostatnich 24 godzin lub działania we wskazanym okresie w ramach domyślnego okresu przechowywania.

Aby zmienić domyślny okres przechowywania, edytuj plik konfiguracyjny task_manager.yaml.

Aby zmienić okres przechowywania

1. Na komputerze z uruchomionym serwerem zarządzania otwórz w edytorze tekstowym następujący plik konfiguracyjny:
   - W systemie Windows: `%Program Files%\Acronis\TaskManager\task_manager.yaml`
   - W systemie Linux: `/usr/lib/Acronis/TaskManager/task_manager.yaml`
2. Odszukaj następującą sekcję:

   ```
   database:
     connection-string: ""
     run-cleanup-at: "23:59"
     cleanup-batch-size: 10
     max-cleanup-retries: 10
     log-queries: false
     max-transaction-retries: 10
     shards:
      - connection-string: sqlite://task-manager.sqlite
        days-to-keep: 90
        space: "default"
        key: "00000000-0000-0000-0000-000000000000"
   ```

3. Edytuj wartość w wierszu `days-to-keep` (okres przechowywania w dniach) stosownie do potrzeb. Na przykład:

   ```
   days-to-keep: 30
   ```

   Uwaga
   Okres przechowywania można zmienić stosownie do swoich potrzeb. Dłuższy okres przechowywania pogarsza wydajność serwera zarządzania.

4. Uruchom ponownie usługę **Acronis Service Manager Service** zgodnie z opisem podanym w sekcji "Aby uruchomić ponownie usługę Acronis Service Manager Service" (s. 204).

Raporty

Program umożliwia korzystanie ze wstępnie zdefiniowanych raportów lub utworzenie raportu niestandardowego. Raport może zawierać dowolny zestaw widżetów pulpitu nawigacyjnego.

Możesz konfigurować raporty tylko w odniesieniu do jednostek, którymi zarządzasz.

Raporty mogą być wysyłane przy użyciu poczty e-mail lub pobierane zgodnie z harmonogramem. Aby wysyłać raporty przy użyciu poczty e-mail, upewnij się, że skonfigurowano ustawienia **serwera poczty e-mail**. Aby przetwarzać raport przy użyciu oprogramowania innego producenta, zaplanuj zapisanie raportu w formacie .xlsx w określonym folderze.

Dostępne raporty zależą od wersji programu Cyber Protect. Raporty domyślne wymieniono poniżej:

Nazwa raportu	Dostępność	Opis
Alerty	Cyber Backup Advanced Cyber Protect Advanced	Umożliwia wyświetlenie alertów zgłoszonych w podanym okresie.
Szczegóły skanowania kopii zapasowej	Cyber Protect Advanced	Umożliwia wyświetlenie szczegółowych informacji o wykrytych zagrożeniach w kopiach zapasowych.
Kopie zapasowe	Cyber Backup Advanced Cyber Protect Advanced	Umożliwia wyświetlenie szczegółowych informacji o bieżących kopiach zapasowych i punktach odzyskiwania.
Aktualny status	Cyber Backup Advanced Cyber Protect Advanced	Umożliwia wyświetlenie bieżącego statusu środowiska.
Codzienne działania	Cyber Backup Advanced Cyber Protect Advanced	Umożliwia wyświetlenie podsumowania działań dotyczących taśm, które zostały wykonane we wskazanym okresie.
Mapa ochrony danych	Cyber Protect Advanced	Umożliwia wyświetlenie szczegółowych informacji o liczbie, rozmiarze, lokalizacji i statusach ochrony wszystkich ważnych plików na komputerach.
Wykryte zagrożenia	Cyber Backup Advanced Cyber Protect	Umożliwia wyświetlenie szczegółowych informacji o zagrożonych komputerach według liczby zablokowanych zagrożeń oraz informacji o komputerach będących w

	Advanced	dobrej kondycji i mających luki w zabezpieczeniach.
Wykryte komputery	Cyber Backup Advanced Cyber Protect Advanced	Umożliwia wyświetlenie listy wszystkich komputerów wykrytych w sieci organizacji.
Prognoza kondycji dysków	Cyber Protect Advanced	Umożliwia wyświetlenie prognozowanych terminów awarii dysków HDD/SSD oraz aktualnych statusów dysków.
Występujące luki w zabezpieczeniach	Cyber Backup Advanced Cyber Protect Advanced	Przedstawia istniejące luki w zabezpieczeniach systemów operacyjnych i aplikacji w Twoim środowisku oraz komputery, których te problemy dotyczą.
Licencje	Cyber Backup Advanced Cyber Protect Advanced	Umożliwia wyświetlenie podsumowania dostępnych licencji.
Lokalizacje	Cyber Backup Advanced Cyber Protect Advanced	Umożliwia wyświetlenie statystyk dotyczących lokalizacji kopii zapasowych w podanym okresie.
Podsumowanie zarządzania poprawkami	Cyber Protect Advanced	Zawiera liczbę brakujących, zainstalowanych i możliwych poprawek. W ramach raportu można wyświetlać bardziej szczegółowe informacje, aby sprawdzać brakujące bądź zainstalowane poprawki oraz informacje na temat wszystkich systemów.
Podsumowanie	Cyber Backup Advanced Cyber Protect Advanced	Umożliwia wyświetlenie podsumowania informacji o chronionych urządzeniach w podanym okresie.
Działania dotyczące taśm	Cyber Backup Advanced Cyber Protect Advanced	Umożliwia wyświetlenie listy taśm używanych w ciągu ostatnich 24 godzin.
Działania w tygodniu	Cyber Backup Advanced Cyber Protect Advanced	Umożliwia wyświetlenie podsumowania działań dotyczących taśm, które zostały wykonane we wskazanym okresie.

Podstawowe operacje dotyczące raportów

- Aby zobaczyć raport, kliknij jego nazwę.
- Aby uzyskać dostęp do kolejnych operacji dotyczących raportu, kliknij ikonę wielokropka (...). Te same operacje są dostępne po otworzeniu raportu.

Aby dodać raport

1. Kliknij **Dodaj raport**.
2. Wykonaj jedną z następujących czynności:
   - Aby zobaczyć wstępnie zdefiniowany raport, kliknij jego nazwę.
   - Aby dodać raport niestandardowy, kliknij **Niestandardowe**. Do listy raportów zostanie dodany nowy raport o nazwie **Niestandardowe**. Otwórz ten raport i dodaj do niego widżety.
3. [Opcjonalnie] Zmień ustawienie widżetów metodą „przeciągnij i upuść".
4. [Opcjonalnie] Edytuj raport zgodnie z poniższymi instrukcjami.

Aby edytować raport

1. Kliknij ikonę wielokropka (...) widoczną obok nazwy raportu, a następnie kliknij **Ustawienia**.
2. Edytuj raport. Użytkownik może:
   - zmianę nazwy raportu,
   - zmianę zakresów czasu wszystkich widżetów w raporcie oraz
   - zaplanowanie wysyłania raportu za pomocą poczty e-mail w formacie .pdf oraz/lub .xlsx.
3. Kliknij **Zapisz**.

Aby zaplanować raport

1. Wybierz raport, a następnie kliknij **Harmonogram**.
2. Włącz przełącznik **Wyślij zaplanowany raport**.
3. Wybierz, czy wysłać raport przy użyciu poczty e-mail, zapisać go w folderze czy wykonać obie czynności. W zależności od dokonanego wyboru określ adresy e-mail, ścieżkę folderu lub jedno i drugie.
4. Wybierz format raportu: .pdf, .xlsx lub oba.
5. Wybierz okres raportowania: 1 dzień, 7 dni lub 30 dni.
6. Wybierz dni i godzinę, kiedy raport będzie wysyłany lub zapisywany.
7. Kliknij **Zapisz**.

Eksportowanie i importowanie struktury raportu

Program pozwala wyeksportować i zaimportować strukturę raportu (zestaw widżetów i ustawienia harmonogramu) do pliku .json. Może to się przydać w razie ponownej instalacji serwera zarządzania lub kopiowania struktury raportu na inny serwer zarządzania.

Aby wyeksportować strukturę raportu, wybierz raport, a następnie kliknij **Eksportuj**.

Aby zaimportować strukturę raportu, kliknij **Utwórz raport**, a następnie kliknij **Importuj**.

Składowanie danych raportu

Program pozwala zapisać zrzut danych raportu w pliku .csv. Zrzut zawiera wszystkie dane raportu (bez filtrowania) dla niestandardowego okresu.

Oprogramowanie generuje zrzut danych na bieżąco. Jeśli określisz długi okres, ta akcja może długo potrwać.

Aby składować dane raportu

1. Wybierz raport, a następnie kliknij **Otwórz**.
2. Kliknij ikonę wielokropka (...) w prawym górnym rogu, a następnie kliknij **Dane zrzutu**.
3. W polu **Lokalizacja** określ ścieżkę folderu pliku .csv.
4. W polu **Zakres czasu** określ przedział czasu.
5. Kliknij **Zapisz**.

Konfigurowanie ważności alertów

Alert to komunikat ostrzegawczy informujący o rzeczywistych lub potencjalnych problemach. Alertów można używać na różne sposoby:

- Sekcja **Alerty** karty **Przegląd** pozwala na szybką identyfikację i rozwiązywanie problemów dzięki monitorowaniu bieżących alertów.
- W obszarze **Urządzenia** stan urządzenia jest określany na podstawie alertów. Kolumna **Stan** umożliwia odfiltrowanie urządzeń z problemami.
- Podczas konfigurowania powiadomień e-mail możesz wybrać alerty wyzwalające powiadomienie.

Alert może przyjmować jedną z następujących ważności:

- **Krytyczny**
- **Błąd**
- **Ostrzeżenie**

Możesz zmienić ważność alertu lub całkowicie wyłączyć alert, w opisany poniżej sposób wykorzystując plik konfiguracji alertów. Ta operacja wymaga ponownego uruchomienia serwera zarządzania.

Zmiana ważności alertu nie wpływa na już wygenerowane alerty.

Plik konfiguracji alertów

Plik konfiguracji znajduje się na komputerze z uruchomionym serwerem zarządzania.

- W systemie Windows: `<ścieżka_instalacji>`**\AlertManager\alert_manager.yaml**
  Tutaj `<ścieżka_instalacji>` to ścieżka instalacji serwera zarządzania. Domyślnie jest to ścieżka: **%ProgramFiles%\Acronis** .
- W systemie Linux: **/usr/lib/Acronis/AlertManager/alert_manager.yaml**

Plik ma strukturę dokumentu YAML. Każdy alert jest pozycją na liście `alertTypes`.

Klucz `name` identyfikuje alert.

Klucz `severity` określa istotność alertu. Musi on przyjmować jedną z następujących wartości: `critical`, `error` lub `warning`.

Opcjonalny klucz `enabled` określa, czy alert jest włączony, czy wyłączony. Musi on mieć wartość `true` lub `false` (prawda lub fałsz). Domyślnie (bez tego klucza) wszystkie alerty są włączone.

Aby zmienić ważność alertu lub wyłączyć alert

1. Na komputerze z zainstalowanym serwerem zarządzania otwórz plik **alert_manager.yaml** w edytorze tekstowym.
2. Znajdź alert, który chcesz zmienić lub wyłączyć.
3. Wykonaj jedną z następujących czynności:
   - Aby zmienić istotność alertu, zmień wartość klucza `severity`.
   - Aby wyłączyć alert, dodaj klucz `enabled`, a następnie ustaw jego wartość na `false`.
4. Zapisz plik.
5. Ponownie uruchom usługę serwera zarządzania w opisany powyżej sposób.

Aby ponownie uruchomić usługę serwera zarządzania w systemie Windows

1. W menu **Start** kliknij **Uruchom**, a następnie wpisz: **cmd**.
2. Kliknij **OK**.
3. Uruchom następujące polecenia:

```
net stop acrmngsrv
net start acrmngsrv
```

Aby ponownie uruchomić usługę serwera zarządzania w systemie Linux

1. Otwórz **Terminal**.
2. W dowolnym katalogu uruchom następujące polecenie:

```
sudo service acronis_ams restart
```

Zaawansowane opcje magazynu

Urządzenia taśmowe

W kolejnych sekcjach szczegółowo opisano korzystanie z urządzeń taśmowych do przechowywania kopii zapasowych.

Co to jest urządzenie taśmowe?

Urządzenie taśmowe to termin ogólny oznaczający bibliotekę taśm lub autonomiczny napęd taśmowy.

Biblioteka taśm (biblioteka automatyczna) to urządzenie pamięci masowej o dużej pojemności, które składa się z:

- jednego lub kilku napędów taśmowych;
- wielu (nawet kilku tysięcy) gniazd do przechowywania taśm;
- jednego lub kilku zmieniaczy (automatów), których zadaniem jest przenoszenie taśm między gniazdami a napędami taśmowymi.

Może ona również obejmować inne komponenty, takie jak czytniki i drukarki kodów kreskowych.

Zmieniacz to szczególna odmiana bibliotek taśm. Składa się z jednego napędu, kilku gniazd, zmieniacza i czytnika kodów kreskowych (opcjonalnie).

Autonomiczny napęd taśmowy (inaczej **streamer**) zawiera jedno gniazdo i umożliwia wsunięcie tylko jednej taśmy w danym czasie.

Omówienie obsługi urządzeń taśmowych

Agenty ochrony mogą tworzyć kopie zapasowe danych na urządzeniu taśmowym bezpośrednio lub za pośrednictwem węzła magazynowania. W obu przypadkach zapewniona jest w pełni automatyczna obsługa urządzenia taśmowego. Jeśli do węzła magazynowania podłączone jest urządzenie taśmowe z kilkoma napędami, możliwe jest jednoczesne tworzenie kopii zapasowych na taśmach za pomocą wielu agentów.

Kompatybilność z oprogramowaniem RSM i programami innych firm

Współistnienie z oprogramowaniem innych firm

Nie można korzystać z taśm na komputerze z zainstalowanym oprogramowaniem innych firm zawierającym zastrzeżone narzędzia do zarządzania taśmami. Aby korzystać z taśm na takim komputerze, musisz odinstalować lub dezaktywować oprogramowanie innych firm do zarządzania taśmami.

Interakcja z menedżerem magazynu wymiennego (RSM) systemu Windows

Agenty ochrony i węzły magazynowania nie używają menedżera RSM. Podczas wykrywania urządzenia taśmowego uniemożliwiają wykorzystanie urządzenia przez menedżera RSM (chyba że jest ono używane przez inne oprogramowanie). Upewnij się, że przez cały czas korzystania z urządzenia taśmowego nie zostanie ono włączone w menedżerze RSM przez użytkownika lub oprogramowanie innych firm. Jeśli urządzenie zostanie włączone w menedżerze RSM, powtórz wykrywanie urządzenia taśmowego.

Obsługiwany sprzęt

Program Acronis Cyber Protect obsługuje zewnętrzne urządzenia SCSI. Są to urządzenia podłączane do sieci Fibre Channel lub używające interfejsów SCSI, iSCSI, Serial Attached SCSI (SAS). Program Acronis Cyber Protect obsługuje również urządzenia taśmowe USB.

W systemie Windows program Acronis Cyber Protect umożliwia tworzenie kopii zapasowych na urządzeniu taśmowym, nawet jeśli nie ma zainstalowanych sterowników zmieniacza urządzenia. Takie urządzenie taśmowe jest pokazywane w oknie **Menedżer urządzeń** jako **Nieznany zmieniacz nośników**. Należy jednak zainstalować sterowniki dysków urządzenia. W przypadku systemu Linux i nośnika startowego utworzenie kopii zapasowej na urządzeniu taśmowym bez sterowników jest niemożliwe.

Nie gwarantuje się możliwości rozpoznawania urządzeń podłączonych do interfejsu IDE lub SATA. Zależy ona od instalacji odpowiednich sterowników w systemie operacyjnym.

Aby sprawdzić, czy dane urządzenie jest obsługiwane, należy skorzystać z narzędzia Hardware Compatibility Tool zgodnie z opisem podanym w artykule http://kb.acronis.com/content/57237. Zachęcamy do wysłania firmie Acronis raportu z wynikami testu. Sprzęt, którego obsługa została potwierdzona, można znaleźć na liście kompatybilności sprzętu: https://go.acronis.com/acronis-cyber-protect-advanced-tape-hcl.

Baza danych zarządzania taśmami

Informacje o wszystkich urządzeniach taśmowych podłączonych do komputera są przechowywane w bazie danych zarządzania taśmami. Domyślna ścieżka bazy danych jest następująca:

- W systemie Windows XP / Server 2003: `%ALLUSERSPROFILE%\Application Data\Acronis\BackupAndRecovery\ARSM\Database`.
- W systemie Windows 7 i nowszych wersjach systemu Windows: `%PROGRAMDATA%\Acronis\BackupAndRecovery\ARSM\Database`.
- W systemie Linux: `/var/lib/Acronis/BackupAndRecovery/ARSM/Database`.

Rozmiar bazy danych zależy od liczby kopii zapasowych przechowywanych na taśmach i wynosi około 10 MB na sto kopii zapasowych. Baza danych może osiągnąć bardzo duży rozmiar, jeśli biblioteka taśm zawiera tysiące kopii zapasowych. W takim przypadku dobrym rozwiązaniem może być zapisanie bazy danych taśm na innym woluminie.

Aby zmienić lokalizację bazy danych w systemie Windows:

1. Zatrzymaj usługę Removable Storage Management.
2. Przenieś wszystkie pliki z lokalizacji domyślnej do nowej.
3. Znajdź klucz rejestru `HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\ARSM\Settings`.
4. Określ ścieżkę nowej lokalizacji w wartości rejestru `ArsmDmlDbProtocol`. Ciąg może zawierać maksymalnie 32 765 znaków.
5. Uruchom usługę Removable Storage Management.

Aby zmienić lokalizację bazy danych w systemie Linux:

1. Zatrzymaj usługę `acronis_rsm`.
2. Przenieś wszystkie pliki z lokalizacji domyślnej do nowej.
3. Otwórz plik konfiguracyjny `/etc/Acronis/ARSM.config` w edytorze tekstowym.
4. Znajdź wiersz `<value name="ArsmDmlDbProtocol" type="TString">`.
5. Zmień ścieżkę w tym wierszu.
6. Zapisz plik.
7. Uruchom usługę `acronis_rsm`.

Folder `TapeLocation`

Folder `TapeLocation` zawiera pamięć podręczną metadanych systemu plików wszystkich woluminów, których kopie zapasowe są tworzone na taśmach.

Domyślna ścieżka folderu `TapeLocation` to:

- W systemie Windows XP / Server 2003: `%ALLUSERSPROFILE%\Application Data\Acronis\BackupAndRecovery\TapeLocation`
- W systemie Windows 7 lub nowszym: `%PROGRAMDATA%\Acronis\BackupAndRecovery\TapeLocation`
- W systemie Linux: `/var/lib/Acronis/BackupAndRecovery/TapeLocation`

Folder `TapeLocation` ma rozmiar równy około 0,5–1% rozmiaru wszystkich kopii zapasowych zapisanych na taśmach. W przypadku kopii zapasowych na poziomie dysku tworzonych przy włączonej opcji odzyskiwania plików folder `TapeLocation` może mieć nieco większy rozmiar, w zależności od liczby plików uwzględnionych w kopiach zapasowych.

Parametry na potrzeby zapisu na taśmach

Parametry zapisu na taśmie (rozmiar bloku i rozmiar pamięci podręcznej) umożliwiają dostosowanie oprogramowania w celu uzyskania maksymalnej wydajności. Do zapisu na taśmie wymagane są oba parametry, ale dostosować trzeba zwykle tylko rozmiar bloku. Optymalna wartość zależy od typu urządzenia taśmowego oraz danych uwzględnianych w kopii zapasowej, takich jak liczba plików i ich rozmiary.

Uwaga
Podczas odczytu z taśmy oprogramowanie stosuje ten sam rozmiar bloku, który został użyty podczas zapisu na taśmie. Jeśli urządzenie taśmowe nie obsługuje danego rozmiaru bloku, odczyt się nie powiedzie.

Parametry ustawia się na każdym komputerze z podłączonym urządzeniem taśmowym. Może to być komputer, na którym jest zainstalowany agent lub węzeł magazynowania. Na komputerze z systemem Windows konfiguracja odbywa się w rejestrze. Na komputerze z systemem Linux określa się ją w pliku konfiguracyjnym **/etc/Acronis/BackupAndRecovery.config**.

W systemie Windows należy utworzyć odpowiednie klucze rejestru i ich wartości DWORD. W systemie Linux należy na końcu pliku konfiguracyjnego, tuż przed znacznikiem `</registry>`, dodać następujący tekst:

```
<key name="TapeLocation">
     <value name="WriteCacheSize" type="Dword">
          "value"
     </value>
     <value name=DefaultBlockSize" type="Dword">
          "value"
     </value>
</key>
```

DefaultBlockSize

Jest to rozmiar bloku (w bajtach) używany podczas zapisu na taśmach.

Możliwe wartości: 0, 32, 64, 128, 256, 512, 1024, 2048, 4096, 8192, 16384, 32768, 65536, 131072, 262144, 524288, 1048576.

Jeśli wartość wynosi 0 lub parametr nie został dodany, rozmiar bloku jest ustalany następująco:

- W systemie Windows wartość jest pobierana ze sterownika urządzenia taśmowego.
- W systemie Linux jest stosowana wartość **64 KB**.

Klucz rejestru (na komputerze z systemem Windows): **HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\BackupAndRecovery\TapeLocation\DefaultBlockSize**

Wiersz tekstu w pliku /etc/Acronis/BackupAndRecovery.config (na komputerze z systemem Linux):

```
     <value name=DefaultBlockSize" type="Dword">
          "value"
     </value>
```

Jeśli określona wartość nie zostanie zaakceptowana przez napęd taśmowy, oprogramowanie będzie ją dzielić przez dwa, aż uzyska odpowiednią wartość lub osiągnie poziom 32 bajtów. Jeśli nie uda się znaleźć odpowiedniej wartości, oprogramowanie będzie mnożyć określoną wartość przez dwa, aż

uzyska odpowiednią wartość lub osiągnie poziom 1 MB. Jeśli napęd nie zaakceptuje żadnej wartości, operacja tworzenia kopii zapasowej się nie powiedzie.

WriteCacheSize

Jest to rozmiar buforu (w bajtach) używany podczas zapisu na taśmach.

Możliwe wartości: 0, 32, 64, 128, 256, 512, 1024, 2048, 4096, 8192, 16384, 32768, 65536, 131072, 262144, 524288, 1048576, ale nie mniej niż wartość parametru **DefaultBlockSize**.

Jeśli wartość wynosi 0 lub parametr nie został dodany, rozmiar buforu ma wartość **1 MB**. Jeśli system operacyjny nie obsługuje tej wartości, oprogramowanie będzie ją dzielić przez dwa, aż znajdzie odpowiednią wartość lub osiągnie poziom wartości parametru **DefaultBlockSize**. Jeśli wartość obsługiwana przez system operacyjny nie zostanie znaleziona, operacja tworzenia kopii zapasowej się nie powiedzie.

Klucz rejestru (na komputerze z systemem Windows):
HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\BackupAndRecovery\TapeLocation\WriteCacheSize

Wiersz tekstu w pliku /etc/Acronis/BackupAndRecovery.config (na komputerze z systemem Linux):

```
<value name="WriteCacheSize" type="Dword">
     "value"
</value>
```

W przypadku określenia wartości niezerowej, która nie jest obsługiwana przez system operacyjny, operacja tworzenia kopii zapasowej się nie powiedzie.

Opcje tworzenia kopii zapasowych związane z taśmami

Można skonfigurować opcje tworzenia kopii zapasowych w sekcji **Zarządzanie taśmami**, które określają:

- czy włączyć odzyskiwanie plików z przechowywanych na taśmach kopii zapasowych na poziomie dysku.
- Czy przenosić taśmy z powrotem do gniazd po zakończeniu wykonywania planu ochrony,
- Czy wysuwać taśmy po ukończeniu tworzenia kopii zapasowej;
- czy używać wolnej taśmy na potrzeby każdej pełnej kopii zapasowej;
- czy zastępować taśmę w napędzie podczas tworzenia pełnej kopii zapasowej (dotyczy tylko autonomicznych napędów taśmowych);
- Czy używać zestawów taśm w celu rozróżniania użytych taśm, na przykład na potrzeby kopii zapasowych tworzonych w inne dni tygodnia lub dla różnych typów komputerów.

Operacje równoległe

Program Acronis Cyber Protect umożliwia równoczesne wykonywanie wielu operacji dotyczących różnych komponentów urządzenia taśmowego. Podczas operacji z użyciem napędu (takiej jak tworzenie kopii zapasowej, odzyskiwanie, ponowne skanowanie lub kasowanie) można uruchomić operację wykorzystującą zmieniacz (przenoszenie taśmy do innego gniazda lub jej wysuwanie) i na odwrót. Jeśli biblioteka taśm składa się z dwóch lub więcej napędów, można także równolegle uruchomić operację korzystającą z jednego z napędów podczas operacji z innym napędem. Na przykład możliwe jest jednoczesne tworzenie kopii zapasowych lub odzyskiwanie na kilku komputerach z użyciem różnych napędów tej samej biblioteki taśm.

Operację wykrywania nowych urządzeń taśmowych można wykonywać równolegle z dowolną inną operacją. Podczas inwentaryzacji nie można wykonywać żadnej innej operacji oprócz wykrywania nowych urządzeń taśmowych.

Operacje, których nie można przeprowadzać równocześnie, są kolejkowane.

Ograniczenia

Korzystanie z urządzenia taśmowego podlega następującym ograniczeniom:

1. Urządzenia taśmowe nie będą obsługiwane, jeśli komputer zostanie uruchomiony z 32-bitowego nośnika startowego opartego na systemie Linux.
2. Na taśmach nie można tworzyć kopii zapasowych następujących typów danych: Skrzynki pocztowe Microsoft 365, skrzynki pocztowe programu Microsoft Exchange.
3. Nie możesz tworzyć uwzględniających aplikacje kopii zapasowych komputerów fizycznych i maszyn wirtualnych.
4. W systemie macOS obsługiwane są tylko kopie zapasowe na poziomie plików tworzone w zarządzanej lokalizacji taśmowej.
5. Nie jest możliwa konsolidacja kopii zapasowych znajdujących się na taśmach. Wskutek tego w przypadku tworzenia kopii zapasowych na taśmach schemat tworzenia kopii zapasowych **Zawsze przyrostowe** jest niedostępny.
6. Nie jest możliwa deduplikacja kopii zapasowych znajdujących się na taśmach.
7. Oprogramowanie nie może automatycznie zastępować danych na taśmie zawierającej nieusunięte kopie zapasowe lub w przypadku istnienia zależnych kopii zapasowych na innych taśmach.

   Jedyny wyjątek od tej reguły jest możliwy w przypadku włączenia opcji „Zastąp taśmę w autonomicznym napędzie taśmowym podczas tworzenia pełnej kopii zapasowej”.
8. Jeśli odzyskiwanie wymaga ponownego uruchomienia systemu operacyjnego, operacji odzyskiwania kopii zapasowej zapisanej na taśmach nie można przeprowadzić pod kontrolą tego systemu. Do tego celu należy użyć nośnika startowego.
9. Możesz sprawdzić poprawność dowolnej kopii zapasowej przechowywanej na taśmach, ale nie możesz wybrać do sprawdzenia poprawności całej lokalizacji taśmowej ani urządzenia taśmowego.

10. Zarządzanej lokalizacji opartej na taśmach nie można zabezpieczyć za pomocą szyfrowania. Zamiast tego zaszyfruj kopie zapasowe.
11. Program nie może jednocześnie zapisywać jednej kopii zapasowej na wielu taśmach ani wielu kopii zapasowych na jednej taśmie za pomocą tego samego napędu taśmowego.
12. Urządzenia korzystające z protokołu NDMP nie są obsługiwane.
13. Nie są obsługiwane drukarki kodów kreskowych.
14. Taśmy sformatowane w systemie Linear Tape File System (LTFS) nie są obsługiwane.

Możliwość odczytu taśm zapisanych przez starsze wersje produktów firmy Acronis

W poniższej tabeli zestawiono możliwości odczytu taśm zapisanych w programach Acronis True Image Echo, Acronis True Image 9.1, Acronis Backup & Recovery 10, Acronis Backup & Recovery 11 oraz produktach z rodzin Acronis Backup 11.5, 11.7 i 12.5 w rozwiązaniu Acronis Cyber Protect. Tabela przedstawia również kompatybilność taśm zapisanych przez różne komponenty programu Acronis Cyber Protect.

Istnieje możliwość dołączania przyrostowych i różnicowych kopii zapasowych do ponownie przeskanowanych kopii zapasowych utworzonych przez programy Acronis Backup 11.5, 11.7 i 12.5.

	...można odczytać przy użyciu urządzenia taśmowego podłączonego do komputera zawierającego...			
	Acronis Cyber Protect Nośnik startowy	Acronis Cyber Protect Agent dla systemu Windows	Acronis Cyber Protect Agent dla systemu Linux	Acronis Cyber Protect Węzeł magazynowania

Taśma zapisana na urządzeniu taśmowym podłączonym lokalnie (napędzie taśmowym lub bibliotece taśm) przez program...	Nośnik startowy	9.1	+	+	+	+
		Echo	+	+	+	+
		ABR10	+	+	+	+
		ABR11/ Acronis Backup 11.5/11.7/12 .5	+	+	+	-
	Agent dla systemu Windows	9.1	+	+	+	+
		Echo	+	+	+	+
		ABR10	+	+	+	+
		ABR11/ Acronis Backup 11.5/11.7/12 .5	+	+	+	-
	Agent dla systemu Linux	9.1	+	+	+	+
		Echo	+	+	+	+
		ABR10	+	+	+	+
		ABR11/ Acronis Backup 11.5/11.7/12 .5	+	+	+	-
Taśma zapisana na urządzeniu taśmowym przez...	Backup Server	9.1	-	-	-	-
		Echo	-	-	-	-
	Węzeł magazynowania	ABR10	+	+	+	+
		ABR11/ Acronis Backup 11.5/11.7/12 .5	+	+	+	+

Rozpoczęcie pracy z urządzeniem taśmowym

Tworzenie kopii zapasowej komputera na lokalnie podłączonym urządzeniu taśmowym

Wymagania wstępne

- Urządzenie taśmowe jest podłączone do komputera zgodnie z instrukcjami producenta.
- Na komputerze jest zainstalowany agent ochrony.

Przed utworzeniem kopii zapasowej

1. Włóż taśmy do urządzenia taśmowego.
2. Zaloguj się do konsoli internetowej Cyber Protect.
3. W obszarze **Ustawienia** > **Zarządzanie taśmami** rozwiń węzeł komputera, a następnie kliknij **Urządzenia taśmowe**.
4. Upewnij się, że jest wyświetlone dołączone urządzenie taśmowe. Jeśli go nie ma, kliknij **Wykryj urządzenia**.
5. Wykonaj inwentaryzację taśm:
   a. Kliknij nazwę urządzenia taśmowego.
   b. Kliknij **Inwentaryzacja** w celu wykrycia załadowanych taśm. **Pełna inwentaryzacja** powinna być włączona. Nie włączaj **Przenieś nierozpoznane lub zaimportowane taśmy do puli „Wolne taśmy”**. Kliknij **Rozpocznij inwentaryzowanie**.
      Rezultat. Załadowane taśmy zostały przeniesione do odpowiednich pul zgodnie z opisem w sekcji „Inwentaryzowanie”.

      Uwaga
      Pełna inwentaryzacja całego urządzenia taśmowego może zabrać dużo czasu.

   c. Jeśli załadowane taśmy zostały przesłane do puli **Nierozpoznane taśmy** lub **Zaimportowane taśmy** i chcesz je wykorzystać do tworzenia kopii zapasowych, przenieś je ręcznie do puli **Wolne taśmy**.

      Uwaga
      Taśmy przesłane do puli **Zaimportowane taśmy** zawierają kopie zapasowe zapisane przez oprogramowanie firmy Acronis. Przed ich przeniesieniem do puli **Wolne taśmy** upewnij się, że nie potrzebujesz już zapisanych na nich kopii zapasowych.

Tworzenie kopii zapasowej

Utwórz plan ochrony zgodnie z opisem w sekcji „Kopia zapasowa”. Podczas określania lokalizacji kopii zapasowej wybierz **Pula taśm „Acronis”**.

Rezultaty

- Aby uzyskać dostęp do lokalizacji, w której zostaną utworzone kopie zapasowe, kliknij **Magazyn kopii zapasowych** > **Pula taśm „Acronis”**.
- Taśmy z kopiami zapasowymi zostaną przeniesione do puli **Acronis**.

Tworzenie kopii zapasowej na urządzeniu taśmowym podłączonym do węzła magazynowania

Wymagania wstępne

- Węzeł magazynowania jest zarejestrowany na serwerze zarządzania.
- Urządzenie taśmowe jest podłączone do węzła magazynowania zgodnie z instrukcjami producenta.

Przed utworzeniem kopii zapasowej

1. Włóż taśmy do urządzenia taśmowego.
2. Zaloguj się do konsoli internetowej Cyber Protect.
3. Kliknij **Ustawienia** > **Zarządzanie taśmami**, rozwiń węzeł z nazwą węzła magazynowania, a następnie kliknij **Urządzenia taśmowe**.
4. Upewnij się, że jest wyświetlone dołączone urządzenie taśmowe. Jeśli go nie ma, kliknij **Wykryj urządzenia**.
5. Wykonaj inwentaryzację taśm:
   a. Kliknij nazwę urządzenia taśmowego.
   b. Kliknij **Inwentaryzacja** w celu wykrycia załadowanych taśm. **Pełna inwentaryzacja** powinna być włączona. Nie włączaj **Przenieś nierozpoznane lub zaimportowane pule taśm do puli „Wolne taśmy”**. Kliknij **Rozpocznij inwentaryzowanie**.
      Rezultat. Załadowane taśmy zostały przeniesione do odpowiednich pul zgodnie z opisem w sekcji „Inwentaryzowanie”.

      Uwaga
      Pełna inwentaryzacja całego urządzenia taśmowego może zabrać dużo czasu.

   c. Jeśli załadowane taśmy zostały przesłane do puli **Nierozpoznane taśmy** lub **Zaimportowane taśmy** i chcesz je wykorzystać do tworzenia kopii zapasowych, przenieś je ręcznie do puli **Wolne taśmy**.

      Uwaga
      Taśmy przesłane do puli **Zaimportowane taśmy** zawierają kopie zapasowe zapisane przez oprogramowanie firmy Acronis. Przed ich przeniesieniem do puli **Wolne taśmy** upewnij się, że nie potrzebujesz już zapisanych na nich kopii zapasowych.

d. Zdecyduj, czy chcesz tworzyć kopie zapasowe w puli **Acronis**, czy też wolisz utworzyć nową pulę.

   Informacje szczegółowe. Posiadanie kilku pul umożliwia używanie osobnego zestawu taśm dla każdego komputera lub działu w firmie. Użycie wielu pul zapobiega wymieszaniu na jednej taśmie kopii zapasowych utworzonych w ramach różnych planów ochrony.

e. Jeśli wybrana pula może w razie potrzeby pobierać taśmy z puli **Wolne taśmy** , pomiń ten krok.

   W przeciwnym razie przenieś taśmy z puli **Wolne taśmy** do wybranej puli.

   Wskazówka. Aby dowiedzieć się, czy pula może pobierać taśmy z puli **Wolne taśmy**, kliknij pulę, a następnie kliknij **Informacja**.

Tworzenie kopii zapasowej

Utwórz plan ochrony zgodnie z opisem w sekcji „Kopia zapasowa”. Podczas określania lokalizacji kopii zapasowej wybierz utworzoną pulę taśm.

Rezultaty

- Aby uzyskać dostęp do lokalizacji, w której zostaną utworzone kopie zapasowe, kliknij **Kopie zapasowe**, a następnie kliknij nazwę utworzonej puli taśm.
- Taśmy z kopiami zapasowymi zostaną przeniesione do wybranej puli.

Wskazówki dotyczące dalszego użycia biblioteki taśm

- Nie trzeba przeprowadzać pełnej inwentaryzacji przy każdym ładowaniu nowej taśmy. W celu zaoszczędzenia czasu postępuj zgodnie z procedurą opisaną w sekcji „Inwentaryzacja” w rozdziale „Połączenie szybkiej i pełnej inwentaryzacji”.
- W tej samej bibliotece taśm można również utworzyć inne pule i wybrać dowolną z nich jako miejsce docelowe kopii zapasowych.

Odzyskiwanie z urządzenia taśmowego pod kontrolą systemu operacyjnego

Aby odzyskiwać dane z urządzenia taśmowego pod kontrolą systemu operacyjnego:

1. Zaloguj się do konsoli internetowej Cyber Protect.
2. Kliknij **Urządzenia**, a następnie wybierz komputer uwzględniony w kopii zapasowej.
3. Kliknij **Odzyskiwanie**.
4. Wybierz punkt odzyskiwania. Uwaga, punkty odzyskiwania są filtrowane na podstawie lokalizacji.
5. W oprogramowaniu zostanie wyświetlona lista taśm wymaganych do przeprowadzenia odzyskiwania. Brakujące taśmy są wyszarzone. Jeśli urządzenie taśmowe ma puste gniazda, włóż te taśmy do urządzenia.
6. Skonfiguruj inne ustawienia odzyskiwania.
7. Kliknij **Rozpocznij odzyskiwanie**, aby rozpocząć operację odzyskiwania.

8. Jeśli którakolwiek z wymaganych taśm z jakiegoś powodu nie została włożona, program wyświetli komunikat z identyfikatorem wymaganej taśmy. Wykonaj następujące czynności:
   a. Włóż taśmę.
   b. Przeprowadź szybką inwentaryzację.
   c. Kliknij **Przegląd** > **Działania**, a następnie kliknij działanie odzyskiwania ze statusem **Wymagane działanie**.
   d. Aby kontynuować odzyskiwanie, kliknij **Pokaż szczegóły**, a następnie kliknij **Ponów**.

Co zrobić, jeśli nie widać kopii zapasowych przechowywanych na taśmach?

Może to oznaczać, że baza danych z zawartością taśm z jakiegoś powodu została utracona lub jest uszkodzona.

Aby odzyskać bazę danych, wykonaj następujące czynności:

1. Przeprowadź szybką inwentaryzację.

   Ostrzeżenie!
   Podczas inwentaryzacji *nie* włączaj przełącznika **Przenieś nierozpoznane i zaimportowane taśmy do puli „Wolne taśmy”**. Włączenie tego przełącznika może spowodować utratę wszystkich kopii zapasowych.

2. Ponownie przeskanuj pulę **Nierozpoznane taśmy**. W jego wyniku odzyskasz zawartość włożonych taśm.
3. Jeśli którakolwiek z wykrytych kopii zapasowych jest kontynuowana na innych taśmach, które nie zostały jeszcze ponownie przeskanowane, po ukazaniu się monitu włóż te taśmy i przeskanuj je ponownie.

Odzyskiwanie pod kontrolą nośnika startowego z lokalnie dołączonego urządzenia taśmowego

Aby odzyskać system pod kontrolą nośnika startowego z lokalnie dołączonego urządzenia taśmowego:

1. Włóż do urządzenia taśmowego taśmy wymagane do przeprowadzenia odzyskiwania.
2. Uruchom komputer za pomocą nośnika startowego.
3. Kliknij **Zarządzaj tym komputerem lokalnie** lub kliknij **Ratunkowy nośnik startowy** dwa razy, w zależności od typu używanego nośnika.
4. Jeśli urządzenie taśmowe jest podłączone za pośrednictwem interfejsu iSCSI, skonfiguruj urządzenie zgodnie z opisem „Konfigurowanie urządzeń iSCSI i NDAS”.
5. Kliknij **Zarządzanie taśmami**.
6. Kliknij **Inwentaryzacja**.
7. W obszarze **Obiekty do zinwentaryzowania** wybierz urządzenie taśmowe.

8. Kliknij **Uruchom**, aby rozpocząć inwentaryzację.
9. Po zakończeniu inwentaryzacji kliknij **Zamknij**.
10. Kliknij **Czynności** > **Odzyskaj**.
11. Kliknij **Wybierz dane**, a następnie kliknij **Przeglądaj**.
12. Rozwiń węzeł **Urządzenia taśmowe**, a następnie wybierz wymagane urządzenie. System wyświetli monit o potwierdzenie ponownego skanowania. Kliknij **Tak**.
13. Wybierz pulę **Nierozpoznane taśmy**.
14. Wybierz taśmy do ponownego skanowania. Aby wybrać wszystkie taśmy z puli, zaznacz pole wyboru obok nagłówka kolumny **Nazwa taśmy**.
15. Jeśli taśmy zawierają kopie zapasowe zabezpieczone hasłem, zaznacz odpowiednie pole wyboru, a następnie wpisz hasło do kopii zapasowych w polu **Hasło**. Jeśli nie podasz hasła albo podane hasło jest niepoprawne, kopie zapasowe nie zostaną wykryte. Pamiętaj o tym w przypadku niewyświetlenia kopii zapasowych po ponownym skanowaniu.

    Wskazówka. Jeśli taśmy zawierają kilka kopii zapasowych zabezpieczonych różnymi hasłami, trzeba kilkakrotnie powtórzyć ponowne skanowanie i za każdym razem podać odpowiednie hasło.
16. Kliknij **Uruchom**, aby uruchomić ponowne skanowanie. W jego wyniku odzyskasz zawartość włożonych taśm.
17. Jeśli którakolwiek z wykrytych kopii zapasowych jest kontynuowana na innych taśmach, które nie zostały jeszcze ponownie przeskanowane, po ukazaniu się monitu włóż te taśmy i przeskanuj je ponownie.
18. Po ukończeniu ponownego skanowania kliknij **OK**.
19. W **Widoku archiwum** wybierz kopię zapasową, której dane chcesz odzyskać, a następnie wybierz dane do odzyskania. Po kliknięciu **OK** na stronie **Odzyskaj dane** zostanie wyświetlona lista taśm wymaganych do przeprowadzenia odzyskiwania. Brakujące taśmy są wyszarzone. Jeśli urządzenie taśmowe ma puste gniazda, włóż te taśmy do urządzenia.
20. Skonfiguruj inne ustawienia odzyskiwania.
21. Kliknij **OK**, aby rozpocząć odzyskiwanie.
22. Jeśli którakolwiek z wymaganych taśm z jakiegoś powodu nie została włożona, program wyświetli komunikat z identyfikatorem wymaganej taśmy. Wykonaj następujące czynności:
    a. Włóż taśmę.
    b. Przeprowadź szybką inwentaryzację.
    c. Kliknij **Przegląd** > **Działania**, a następnie kliknij działanie odzyskiwania ze statusem **Wymagane działanie**.
    d. Aby kontynuować odzyskiwanie, kliknij **Pokaż szczegóły**, a następnie kliknij **Ponów**.

Odzyskiwanie danych za pomocą nośnika startowego z urządzenia taśmowego dołączonego do węzła magazynowania

Aby odzyskać dane za pomocą nośnika startowego z urządzenia taśmowego dołączonego do węzła magazynowania:

1. Włóż do urządzenia taśmowego taśmy wymagane do przeprowadzenia odzyskiwania.
2. Uruchom komputer za pomocą nośnika startowego.
3. Kliknij **Zarządzaj tym komputerem lokalnie** lub kliknij **Ratunkowy nośnik startowy** dwa razy, w zależności od typu używanego nośnika.
4. Kliknij **Odzyskaj**.
5. Kliknij **Wybierz dane**, a następnie kliknij **Przeglądaj**.
6. W polu **Ścieżka** wpisz `bsp://<adres wezla magazynowania>/<nazwa puli>/`, gdzie `<adres wezla magazynowania>` to adres IP węzła magazynowania zawierającego wymaganą kopię zapasową, a `<nazwa puli>` to nazwa puli taśm. Kliknij **OK** i określ poświadczenia do puli.
7. Wybierz kopię zapasową, a następnie wybierz dane, które chcesz odzyskać. Po kliknięciu **OK** na stronie **Odzyskaj dane** zostanie wyświetlona lista taśm wymaganych do przeprowadzenia odzyskiwania. Brakujące taśmy są wyszarzone. Jeśli urządzenie taśmowe ma puste gniazda, włóż te taśmy do urządzenia.
8. Skonfiguruj inne ustawienia odzyskiwania.
9. Kliknij **OK**, aby rozpocząć odzyskiwanie.
10. Jeśli którakolwiek z wymaganych taśm z jakiegoś powodu nie została włożona, program wyświetli komunikat z identyfikatorem wymaganej taśmy. Wykonaj następujące czynności:
    a. Włóż taśmę.
    b. Przeprowadź szybką inwentaryzację.
    c. Kliknij **Przegląd** > **Działania**, a następnie kliknij działanie odzyskiwania ze statusem **Wymagane działanie**.
    d. Aby kontynuować odzyskiwanie, kliknij **Pokaż szczegóły**, a następnie kliknij **Ponów**.

Zarządzanie taśmami

Wykrywanie urządzeń taśmowych

W trakcie procedury wykrywania urządzeń taśmowych program do tworzenia kopii zapasowych znajduje wszystkie urządzenia taśmowe podłączone do komputera i umieszcza związane z nimi informacje w bazie danych zarządzania taśmami. Wykryte urządzenia taśmowe są wyłączane w RSM.

Zazwyczaj urządzenie taśmowe jest wykrywane automatycznie po jego podłączeniu do komputera z zainstalowanym produktem. Jednak w następujących przypadkach może być konieczne wykrycie urządzeń taśmowych:

- Po podłączeniu lub ponownym podłączeniu urządzenia taśmowego.
- Po zainstalowaniu lub ponownym zainstalowaniu programu do tworzenia kopii zapasowych na komputerze, do którego jest podłączone urządzenie taśmowe.

Aby wykryć urządzenia taśmowe

1. Kliknij **Ustawienia** > **Zarządzanie taśmami**.
2. Wybierz komputer, do którego jest podłączone urządzenie taśmowe.
3. Kliknij **Wykryj urządzenia**. Zostaną wyświetlone informacje o podłączonych urządzeniach taśmowych, ich napędach i gniazdach.

Pule taśm

Program do tworzenia kopii zapasowych korzysta z pul taśm będących logicznymi grupami taśm. Zawiera on następujące wstępnie zdefiniowane pule taśm: **Nierozpoznane taśmy**, **Zaimportowane taśmy**, **Wolne taśmy** i **Acronis**. Można również tworzyć własne, niestandardowe pule.

Pula **Acronis** i pule niestandardowe są również używane jako lokalizacje kopii zapasowych.

Wstępnie zdefiniowane pule

Nierozpoznane taśmy

Pula zawiera taśmy, które były zapisane przez aplikacje innych firm. Aby móc na nich zapisywać, należy je jawnie przenieść do puli **Wolne taśmy**. Taśm z tej puli nie można przenosić do żadnej innej puli niż **Wolne taśmy**.

Zaimportowane taśmy

Pula zawiera taśmy zapisane przez program Acronis Cyber Protect na urządzeniu taśmowym podłączonym do innego węzła magazynowania lub agenta. Aby móc na nich zapisywać, należy je jawnie przenieść do puli **Wolne taśmy**. Taśm z tej puli nie można przenosić do żadnej innej puli niż **Wolne taśmy**.

Wolne taśmy

Pula zawiera wolne (puste) taśmy. Taśmy z tej puli można ręcznie przenosić do innych pul.

W przypadku przenoszenia taśmy do puli **Wolne taśmy** oprogramowanie oznaczy ją jako pustą. Jeśli taśma zawiera kopie zapasowe, są one oznaczone ikoną  . Kiedy oprogramowanie rozpoczyna zastępowanie danych na taśmie, dane dotyczące kopii zapasowych zostaną usunięte z bazy danych.

Acronis

Pula służy domyślnie do tworzenia kopii zapasowych, jeśli użytkownik nie chce utworzyć własnych pul. Zwykle odnosi się ona do pojedynczego napędu z niewielką liczbą taśm.

Pule niestandardowe

Jeśli chcesz oddzielić kopie zapasowe różnych danych, musisz utworzyć kilka pul. Warto na przykład utworzyć niestandardowe pule w celu oddzielenia:

- kopii zapasowych pochodzących z poszczególnych działów firmy;
- kopii zapasowych poszczególnych komputerów;
- kopii zapasowych woluminów systemowych i danych użytkowników.

Operacje dotyczące pul

Tworzenie puli

Aby utworzyć pulę:

1. Kliknij opcję **Ustawienia** > **Zarządzanie taśmami**.
2. Wybierz komputer lub węzeł magazynowania, do którego jest podłączone urządzenie taśmowe, a następnie na tym komputerze kliknij opcję **Pule taśm**.
3. Kliknij **Utwórz pulę**.
4. Określ nazwę puli.
5. [Opcjonalnie] Usuń zaznaczenie pola wyboru **W razie potrzeby automatycznie pobieraj taśmy z puli wolnych taśm**. Jeśli pole to nie jest zaznaczone, do tworzenia kopii zapasowych będą użyte tylko te taśmy, które w określonym momencie znajdują się w nowej puli.
6. Kliknij **Utwórz**.

Edycja puli

Możesz edytować parametry puli **Acronis** lub własnej puli niestandardowej.

Aby wyedytować pulę:

1. Kliknij opcję **Ustawienia** > **Zarządzanie taśmami**.
2. Wybierz komputer lub węzeł magazynowania, do którego jest podłączone urządzenie taśmowe, a następnie na tym komputerze kliknij opcję **Pule taśm**.
3. Wybierz żądaną pulę, a następnie kliknij **Edytuj pulę**.
4. Możesz zmienić nazwę puli lub jej ustawienia. Aby uzyskać więcej informacji o ustawieniach pul, zobacz „Tworzenie puli”.
5. Kliknij opcję **Zapisz**, aby zapisać zmiany.

Usuwanie puli

Program umożliwia usuwanie tylko pul niestandardowych. Wstępnie zdefiniowanych pul taśm (**Nierozpoznane taśmy**, **Zaimportowane taśmy**, **Wolne taśmy** i **Acronis**) nie można usunąć.

Uwaga
Po usunięciu puli koniecznie zmodyfikuj plany ochrony, w których tę pulę zdefiniowano jako lokalizację kopii zapasowych. Jeśli tego nie zrobisz, nie uda się wykonać tych planów ochrony.

Aby usunąć pulę:

1. Kliknij opcję **Ustawienia** > **Zarządzanie taśmami**.
2. Wybierz komputer lub węzeł magazynowania, do którego jest podłączone urządzenie taśmowe, a następnie na tym komputerze kliknij opcję **Pule taśm**.
3. Wybierz żądaną pulę i kliknij **Usuń**.
4. Wybierz pulę, do której zostaną przeniesione taśmy z usuwanej puli po jej usunięciu.
5. Kliknij **OK**, aby usunąć pulę.

Operacje na taśmach

Przenoszenie do innego gniazda

Zastosuj tę operację w następujących sytuacjach:

- Musisz wyjąć jednocześnie kilka taśm z urządzenia taśmowego.
- Urządzenie taśmowe nie jest wyposażone w gniazdo poczty, a wyjmowane taśmy znajdują się w gniazdach magazynków niewymiennych.

Musisz przenieść taśmy do gniazd jednego magazynka, a następnie ręcznie wyjąć magazynek.

Aby przenieść taśmę do innego gniazda:

1. Kliknij opcję **Ustawienia** > **Zarządzanie taśmami**.
2. Wybierz komputer lub węzeł magazynowania, do którego jest podłączone urządzenie taśmowe, a następnie na tym komputerze kliknij opcję **Pule taśm**.
3. Kliknij pulę zawierającą wymaganą taśmę, a następnie wybierz żądaną taśmę.
4. Kliknij opcję **Przenieś do gniazda**.
5. Wybierz nowe gniazdo, do którego chcesz przenieść wybraną taśmę.
6. Kliknij opcję **Przenieś**, aby rozpocząć operację.

Przenoszenie do innej puli

Ta operacja służy do przenoszenia jednej lub kilku taśm z jednej puli do drugiej.

W przypadku przenoszenia taśmy do puli **Wolne taśmy** oprogramowanie oznaczy ją jako pustą. Jeśli taśma zawiera kopie zapasowe, są one oznaczone ikoną  . Kiedy oprogramowanie rozpoczyna zastępowanie danych na taśmie, dane dotyczące kopii zapasowych zostaną usunięte z bazy danych.

Uwagi dotyczące określonych typów taśm

- Do puli **Wolne taśmy** nie można przenosić taśm zabezpieczonych przed zapisem ani taśm jednokrotnego zapisu WORM (ang. Write-Once-Read-Many).
- Taśmy czyszczące są zawsze wyświetlane w puli **Nierozpoznane taśmy** i nie można ich przenieść do innej puli.

Aby przenieść taśmy do innej puli:

1. Kliknij opcję **Ustawienia** > **Zarządzanie taśmami**.
2. Wybierz komputer lub węzeł magazynowania, do którego jest podłączone urządzenie taśmowe, a następnie na tym komputerze kliknij opcję **Pule taśm**.
3. Kliknij pulę zawierającą wymagane taśmy, a następnie wybierz żądane taśmy.
4. Kliknij opcję **Przenieś do puli**.
5. [Opcjonalnie] Kliknij opcję **Utwórz nową pulę**, jeśli chcesz utworzyć kolejną pulę dla wybranych taśm. Wykonaj czynności opisane w sekcji „Tworzenie puli”.
6. Wybierz pulę, do której chcesz przenieść taśmy.
7. Kliknij opcję **Przenieś**, aby zapisać zmiany.

Uwaga
Jeśli na taśmie znajdują się kopie zapasowe, które można przywrócić, i taśma ta jest przenoszona do innej puli, po zakończeniu operacji przeniesienia koniecznie odśwież skarbiec w sekcji Magazyn kopii zapasowych. Te kopie zapasowe będą dostępne w drugiej puli mimo pierwotnego miejsca docelowego kopii zapasowych.

Inwentaryzacja

Operacja inwentaryzacji wykrywa taśmy załadowane w urządzeniu taśmowym i przypisuje nazwy jeszcze nienazwanym taśmom.

Metody inwentaryzacji

Istnieją dwie metody inwentaryzacji.

Szybka inwentaryzacja

Agent lub węzeł magazynowania skanuje taśmy w poszukiwaniu kodów kreskowych. Dzięki stosowaniu kodów kreskowych oprogramowanie może szybko zwrócić taśmę do puli, z której ona pochodzi.

Ta metoda umożliwia rozpoznawanie taśm używanych przez to samo urządzenie taśmowe podłączone do tego samego komputera. Inne taśmy zostaną wysłane do puli **Nierozpoznane taśmy**.

Jeśli biblioteka taśm nie jest wyposażona w czytnik kodów kreskowych, wszystkie taśmy zostaną wysłane do puli **Nierozpoznane taśmy**. W celu rozpoznania taśm należy przeprowadzić pełną inwentaryzację lub zastosować połączenie szybkiej i pełnej inwentaryzacji w sposób opisany w dalszej części tej sekcji.

Pełna inwentaryzacja

Agent lub węzeł magazynowania odczytuje wcześniej zapisane znaczniki oraz analizuje inne informacje o zawartości załadowanych taśm. Wybór tej metody umożliwia rozpoznawanie pustych taśm i taśm zapisanych przez to samo oprogramowanie na dowolnym urządzeniu taśmowym i dowolnym komputerze.

W poniższej tabeli znajdują się pule, do których w wyniku pełnej inwentaryzacji są wysyłane taśmy.

Taśma była używana przez...	Taśma jest odczytywana przez...	Taśma jest wysyłana do puli...
Agent	Tego samego agenta	W której znajdowała się wcześniej
	Inny agent	**Zaimportowane taśmy**
	Węzeł magazynowania	**Zaimportowane taśmy**
Węzeł magazynowania	Ten sam węzeł magazynowania	W której znajdowała się wcześniej
	Inny węzeł magazynowania	**Zaimportowane taśmy**
	Agent	**Zaimportowane taśmy**
Aplikację innej firmy do tworzenia kopii zapasowych	Agenta lub węzeł magazynowania	**Nierozpoznane taśmy**

Taśmy pewnych typów są wysyłane do określonych pul:

Typ taśmy	Taśma jest wysyłana do puli...
Pusta taśma	**Wolne taśmy**
Pusta taśma zabezpieczona przed zapisem	**Nierozpoznane taśmy**
Taśma czyszcząca	**Nierozpoznane taśmy**

Szybką inwentaryzację można stosować do całych urządzeń taśmowych. Pełną inwentaryzację można stosować do całych urządzeń taśmowych, pojedynczych napędów oraz gniazd. W przypadku autonomicznych napędów taśmowych pełna inwentaryzacja jest zawsze przeprowadzana, nawet gdy zostanie wybrana szybka inwentaryzacja.

Połączenie szybkiej i pełnej inwentaryzacji

Pełna inwentaryzacja całego urządzenia taśmowego może zabrać dużo czasu. Jeśli zinwentaryzowania wymaga tylko kilka taśm, wykonaj następujące czynności:

1. Przeprowadź szybką inwentaryzację urządzenia taśmowego.
2. Kliknij pulę **Nierozpoznane taśmy**. Znajdź taśmy do inwentaryzacji i zapisz, które gniazda one

zajmują.

3. Przeprowadź pełną inwentaryzację tych gniazd.

Co zrobić po inwentaryzacji

Jeśli chcesz tworzyć kopie zapasowe na taśmach znajdujących się w puli **Nierozpoznane taśmy** lub **Zaimportowane taśmy**, przenieś je do puli **Wolne taśmy**, a następnie do puli **Acronis** lub puli niestandardowej. Jeśli pula, w której chcesz tworzyć kopie zapasowe, umożliwia uzupełnianie, możesz pozostawić taśmy w puli **Wolne taśmy**.

Jeśli chcesz odzyskać dane z taśmy znajdującej się w puli **Nierozpoznane taśmy** lub **Zaimportowane taśmy**, musisz ją ponownie przeskanować. Taśma zostanie przeniesiona do puli wybranej podczas ponownego skanowania, a kopie zapasowe przechowywane na taśmie pojawią się w tej lokalizacji.

Kolejność czynności

1. Kliknij opcję **Ustawienia** > **Zarządzanie taśmami**.
2. Wybierz komputer , do którego jest podłączone urządzenie taśmowe, a następnie wybierz urządzenie taśmowe, które chcesz zinwentaryzować.
3. Kliknij **Inwentaryzacja**.
4. [Opcjonalnie] Aby wybrać szybką inwentaryzację, wyłącz opcję **Pełna inwentaryzacja**.
5. [Opcjonalnie] Włącz opcję **Przenieś nierozpoznane i zaimportowane taśmy do puli „Wolne taśmy”**.

   Ostrzeżenie!
   Ten przełącznik należy włączyć tylko, gdy masz absolutną pewność, że dane zapisane na taśmach mogą zostać zastąpione.

6. Kliknij **Rozpocznij inwentaryzowanie teraz**, aby rozpocząć inwentaryzację.

Ponowne skanowanie

Informacje o zawartości taśm są przechowywane w specjalnej bazie danych. Operacja ponownego skanowania powoduje odczyt zawartości taśm i aktualizację bazy danych, jeśli informacje w niej nie odpowiadają danym przechowywanym na taśmach. Kopie zapasowe wykryte w wyniku tej operacji zostaną umieszczone w określonej puli.

W czasie jednej operacji można ponownie skanować taśmy z jednej puli. Operacja jest możliwa tylko w odniesieniu do taśm w trybie online.

Do ponownego przeskanowania taśm z kopią zapasową utworzoną przy użyciu wielu strumieni lub multipleksową kopią zapasową potrzeba co najmniej tylu napędów, ilu użyto do utworzenia tej kopii. Tego typu kopii zapasowej nie można przeskanować za pomocą autonomicznego napędu taśmowego.

Uruchom ponowne skanowanie:

- Jeśli baza danych węzła magazynowania lub komputera zarządzanego została utracona lub uległa uszkodzeniu.
- Jeśli informacje o taśmie zapisane w bazie danych są nieaktualne (zawartość taśmy została na przykład zmodyfikowana przez innego agenta lub węzeł magazynowania).
- Aby uzyskać dostęp do kopii zapasowych przechowywanych na taśmach z poziomu nośnika startowego.
- Jeśli przypadkowo usunięto z bazy danych informacje na temat taśmy. Po ponownym przeskanowaniu usuniętej taśmy przechowywane na niej kopie zapasowe znów pojawią się w bazie danych i staną się dostępne do odzyskania.
- Jeśli kopie zapasowe zostały usunięte z taśmy ręcznie lub za pośrednictwem reguł przechowywania, ale chcesz je udostępnić do operacji odzyskiwania danych. Przed ponownym skanowaniem takiej taśmy wysuń ją, usuń z bazy danych informacje jej dotyczące, a następnie ponownie włóż taśmę do urządzenia taśmowego.

Aby ponownie przeskanować taśmy:

1. Kliknij opcję **Ustawienia** > **Zarządzanie taśmami**.
2. Wybierz komputer lub węzeł magazynowania, do którego jest podłączone urządzenie taśmowe, a następnie w obszarze tego komputera kliknij **Urządzenia taśmowe**.
3. Wybierz urządzenie taśmowe, do którego załadowano taśmy.
4. Przeprowadź szybką inwentaryzację.

   Uwaga
   Podczas inwentaryzacji *nie* włączaj przełącznika **Przenieś nierozpoznane i zaimportowane taśmy do puli „Wolne taśmy”**.

5. Wybierz pulę **Nierozpoznane taśmy**. Jest to pula, do której wysyłana jest większość taśm nagranych w wyniku szybkiej inwentaryzacji. Możliwe jest także ponowne skanowanie dowolnej innej puli.
6. [Opcjonalnie] Aby ponownie przeskanować tylko poszczególne taśmy, wybierz je.
7. Kliknij **Skanuj ponownie**.
8. Wybierz pulę, w której zostaną umieszczone nowo wykryte kopie zapasowe.
9. W razie potrzeby zaznacz pole wyboru **Włącz odzyskiwanie plików z kopii zapasowych dysków przechowywanych na taśmach**.

   Informacje szczegółowe. Jeśli to pole wyboru jest zaznaczone, program utworzy specjalne pliki pomocnicze na dysku twardym komputera, do którego jest podłączone urządzenie taśmowe. Odzyskiwanie plików z kopii zapasowych dysków będzie możliwe pod warunkiem, że te pliki pomocnicze pozostaną nienaruszone. Nie zapomnij zaznaczyć tego pola wyboru, jeśli taśmy zawierają kopie zapasowe uwzględniające aplikacje. W innym przypadku nie będzie można odzyskać danych aplikacji z tych kopii zapasowych.
10. Jeśli taśmy zawierają kopie zapasowe zabezpieczone hasłem, zaznacz odpowiednie pole wyboru, a następnie określ hasło do kopii zapasowych. Jeśli nie określisz hasła albo wprowadzisz

niepoprawne hasło, kopie zapasowe nie zostaną wykryte. Pamiętaj o tym w przypadku niewyświetlenia kopii zapasowych po ponownym skanowaniu.

Wskazówka. Jeśli taśmy zawierają kopie zapasowej zabezpieczone różnymi hasłami, trzeba kilkakrotnie powtórzyć ponowne skanowanie, za każdym razem określając odpowiednie hasło.

11. Kliknij **Uruchom ponowne skanowanie**, aby uruchomić ponowne skanowanie.

Rezultat. Wybrane taśmy zostały przeniesione do wybranej puli. Zawiera ona kopie zapasowe przechowywane na tych taśmach. Kopia zapasowa znajdująca się na kilku taśmach nie pojawi się w puli, dopóki wszystkie te taśmy nie zostaną ponownie przeskanowane.

Zmiana nazwy

Po wykryciu taśmy przez program jest jej automatycznie przypisywana nazwa w następującym formacie: **Taśma XXX**, gdzie **XXX** to unikatowy numer. Taśmom są nadawane kolejne numery. Operacja zmiany nazwy umożliwia ręczną zmianę nazwy taśmy.

Aby zmienić nazwy taśm:

1. Kliknij opcję **Ustawienia** > **Zarządzanie taśmami**.
2. Wybierz komputer lub węzeł magazynowania, do którego jest podłączone urządzenie taśmowe, a następnie na tym komputerze kliknij opcję **Pule taśm**.
3. Kliknij pulę zawierającą wymaganą taśmę, a następnie wybierz żądaną taśmę.
4. Kliknij **Zmień nazwę**.
5. Wpisz nową nazwę wybranej taśmy.
6. Kliknij **Zmień nazwę**, aby zapisać zmiany.

Kasowanie

Skasowanie zawartości taśmy powoduje fizyczne usunięcie wszystkich przechowywanych na niej kopii zapasowych oraz usunięcie informacji o tych kopiach z bazy danych. Informacja o samej taśmie pozostanie jednak w bazie danych.

Po skasowaniu taśma znajdująca się w puli **Nierozpoznane taśmy** lub **Zaimportowane taśmy** jest przenoszona do puli **Wolne taśmy**. Taśmy z innych pul nie będą przenoszone.

Aby wykasować taśmy:

1. Kliknij opcję **Ustawienia** > **Zarządzanie taśmami**.
2. Wybierz komputer lub węzeł magazynowania, do którego jest podłączone urządzenie taśmowe, a następnie na tym komputerze kliknij opcję **Pule taśm**.
3. Kliknij pulę zawierającą wymagane taśmy, a następnie wybierz żądane taśmy.
4. Kliknij **Kasuj**. System wyświetli monit z prośbą o potwierdzenie operacji.
5. Wybierz metodę kasowania: szybka lub pełna.
6. Kliknij **Kasuj**, aby rozpocząć operację.

   Informacje szczegółowe. Operacji kasowania nie można anulować.

Wysuwanie

Aby pomyślnie wysunąć taśmę z biblioteki taśm, biblioteka musi być wyposażona w gniazdo poczty, które nie może być zablokowane przez użytkownika lub inne oprogramowanie.

Aby wysunąć taśmy:

1. Kliknij opcję **Ustawienia** > **Zarządzanie taśmami**.
2. Wybierz komputer lub węzeł magazynowania, do którego jest podłączone urządzenie taśmowe, a następnie na tym komputerze kliknij opcję **Pule taśm**.
3. Kliknij pulę zawierającą wymagane taśmy, a następnie wybierz żądane taśmy.
4. Kliknij **Wysuń**. Program wyświetli monit o podanie opisu taśmy. Zalecamy opisanie fizycznej lokalizacji, gdzie taśmy będą przechowywane. Oprogramowanie wyświetli ten opis w trakcie odzyskiwania, aby można było łatwo odnaleźć taśmy.
5. Kliknij **Wysuń**, aby rozpocząć operację.

Po ręcznym lub automatycznym wysunięciu taśmy zaleca się umieszczenie na niej jej nazwy.

Usuwanie

Operacja usuwania usuwa z bazy danych informacje na temat kopii zapasowych przechowywanych na wybranej taśmie oraz dotyczące samej taśmy.

Usuwać można tylko taśmy w trybie offline (wysunięte).

Aby usunąć taśmę:

1. Kliknij opcję **Ustawienia** > **Zarządzanie taśmami**.
2. Wybierz komputer lub węzeł magazynowania, do którego jest podłączone urządzenie taśmowe, a następnie na tym komputerze kliknij opcję **Pule taśm**.
3. Kliknij pulę zawierającą wymaganą taśmę, a następnie wybierz żądaną taśmę.
4. Kliknij **Usuń**. System wyświetli monit z prośbą o potwierdzenie operacji.
5. Kliknij **Usuń**, aby usunąć taśmę.

Co zrobić w przypadku przypadkowego usunięcia taśmy?

W odróżnieniu od taśmy skasowanej dane z taśmy usuniętej nie są fizycznie usuwane. Z tego względu kopie zapasowe przechowywane na takiej taśmie można ponownie udostępnić. W tym celu:

1. Załaduj taśmę do urządzenia taśmowego.
2. Przeprowadź szybką inwentaryzację w celu wykrycia taśmy.

Uwaga
Podczas inwentaryzacji *nie* włączaj przełącznika **Przenieś nierozpoznane i zaimportowane taśmy do puli „Wolne taśmy”**.

3. Wykonaj ponowne skanowanie, aby dopasować dane przechowywane na taśmach do informacji w bazie danych.

Określanie zestawu taśm

Ta operacja umożliwia określenie zestawu taśm.

Zestaw taśm to grupa taśm w jednej puli.

W przeciwieństwie do określania zestawów taśm w opcjach tworzenia kopii zapasowej, gdzie można używać zmiennych, tutaj można określić tylko wartość ciągu.

Wykonanie tej operacji spowoduje, że oprogramowanie będzie wykonywać kopie zapasowe na *określonych* taśmach według ustalonej reguły — pozwala na przykład przechowywać kopie zapasowe z poniedziałku na taśmie 1, z wtorku na taśmie 2 itd. Określ zestawy taśm dla poszczególnych wymaganych taśm, a następnie określ ten sam zestaw taśm lub użyj zmiennych w opcjach tworzenia kopii zapasowych.

W powyższym przykładzie można wybrać zestaw taśm `Poniedziałek` dla taśmy 1, `Wtorek` dla taśmy 2 itd. W opcjach tworzenia kopii zapasowej określ parametr `[dzień tygodnia]`. Dzięki temu w danym dniu tygodnia będzie używana odpowiednia taśma.

Aby określić zestaw taśm obejmujący taśmę lub kilka taśm:

1. Kliknij opcję **Ustawienia** > **Zarządzanie taśmami**.
2. Wybierz komputer lub węzeł magazynowania, do którego jest podłączone urządzenie taśmowe, a następnie na tym komputerze kliknij opcję **Pule taśm**.
3. Kliknij pulę zawierającą wymagane taśmy, a następnie wybierz żądane taśmy.
4. Kliknij opcję **Zestaw taśm**.
5. Wpisz nazwę zestawu taśm. Jeśli dla wybranych taśm określono już inny zestaw taśm, zostanie on zastąpiony. Aby wykluczyć taśmy z zestawu taśm, nie wybierając innego, usuń nazwę istniejącego zestawu taśm.
6. Kliknij opcję **Zapisz**, aby zapisać zmiany.

Węzły magazynowania

Węzeł magazynowania to serwer przeznaczony do optymalizacji użycia różnych zasobów (takich jak pojemność magazynu firmowego, przepustowości sieci i obciążenia procesorów serwerów produkcyjnych) wymaganych do ochrony danych przedsiębiorstwa. Cel ten jest osiągany dzięki organizowaniu lokalizacji służących jako dedykowane magazyny kopii zapasowych przedsiębiorstwa (lokalizacje zarządzane) i zarządzaniu nimi.

Głównym zadaniem narzędzia Acronis Storage Node jest umożliwienie scentralizowanego dostępu do napędów taśmowych lub bibliotek taśm, na przykład w celu tworzenia kopii zapasowych i odzyskiwania danych z wielu urządzeń na tym samym napędzie taśmowym lub tej samej bibliotece taśm (skarbcu zarządzanym na taśmie).

Innym zastosowaniem jest włączenie zaawansowanych funkcji deduplikacji, w przypadku których dane z wielu urządzeń muszą być deduplikowane względem siebie i przechowywane w jednej lokalizacji (skarbcu zarządzanym z włączoną deduplikacją).

Instalowanie węzła magazynowania i usługi wykazu

Przed instalacją węzła magazynowania upewnij się, że komputer spełnia wymagania systemowe.

Zalecamy zainstalowanie węzła magazynowania i usługi wykazu na oddzielnych komputerach. Wymagania systemowe dotyczące komputera z usługą wykazu opisano w sekcji "Sprawdzone praktyki dotyczące katalogowania" (s. 652).

Aby zainstalować węzeł magazynowania i/lub usługę wykazu

1. Zaloguj się jako administrator i uruchom program instalacyjny produktu Acronis Cyber Protect.
2. [Opcjonalnie] Aby zmienić język programu instalacyjnego, kliknij **Skonfiguruj język**.
3. Zaakceptuj warunki umowy licencyjnej i zasady ochrony prywatności, a następnie kliknij **Kontynuuj**.
4. Kliknij **Zainstaluj agenta ochrony**.
5. Kliknij **Dostosuj ustawienia instalacji**.
6. Obok pozycji **Elementy do zainstalowania** kliknij **Zmień**.
7. Wybierz komponenty do zainstalowania:
   - Aby zainstalować węzeł magazynowania, zaznacz pole wyboru **Węzeł magazynowania**. Pole wyboru **Agent dla systemu Windows** jest zaznaczone automatycznie.
   - Aby zainstalować usługę wykazu, zaznacz pole wyboru **Usługa wykazu**.
   - Jeśli nie chcesz instalować na komputerze innych komponentów, usuń zaznaczenia odpowiednich pól wyboru.

   Kliknij **Gotowe**, aby kontynuować.
8. Określ serwer zarządzania, na którym zostaną zarejestrowane komponenty:
   a. Kliknij Określ obok pozycji **Acronis Cyber Protect Management Server**.
   b. Określ nazwę hosta lub adresIP komputera, na którym jest zainstalowany serwer zarządzania.
   c. Podaj poświadczenia administratora serwera zarządzania lub token rejestracji.
      Dodatkowe informacje o procedurze generowania tokenu rejestracji można znaleźć w sekcji "Krok 1: Generowanie tokenu rejestracji" (s. 183).
   d. Kliknij **Gotowe**.
9. Jeśli pojawi się monit, wybierz, czy komputer z węzłem magazynowania i/lub usługą wykazu zostanie dodany do organizacji, czy do jednej z jednostek.
   Monit pojawia się w sytuacji, gdy administrujesz więcej niż jedną jednostką lub organizacją mającą co najmniej jedną jednostkę. W przeciwnym razie komputer zostanie dodany w trybie dyskretnym do administrowanej jednostki lub organizacji. Aby uzyskać więcej informacji, zobacz „Administratorzy i jednostki”.

10. [Opcjonalnie] Zmień inne ustawienia instalacji zgodnie z opisem podanym w sekcji „Dostosowywanie ustawień instalacji”.
11. Kliknij **Zainstaluj**, aby kontynuować instalację.
12. Po zakończeniu instalacji kliknij **Zamknij**.

Aktualizowanie usługi wykazu przy użyciu rozwiązania Acronis Cyber Protect 15 Update 4

Rozwiązanie Acronis Cyber Protect 15 Update 4 korzysta z nowej wersji usługi wykazu. Nowa wersja nie jest bezpośrednio zgodna z danymi wykazu utworzonymi przez starsze wersje.

Podczas aktualizowania do rozwiązania Acronis Cyber Protect 15 Update 4 można ręcznie przeprowadzić migrację tych danych do nowej wersji usługi wykazu. Można też pominąć migrację i odtworzyć dane wykazu później. Odtworzenie danych wykazu trwa dłużej niż ich migracja.

Aby przeprowadzić migrację danych wykazu

1. Na komputerze z zainstalowaną usługą wykazu uruchom program instalacyjny rozwiązania Acronis Cyber Protect.
2. Zaakceptuj warunki umowy licencyjnej i zasady ochrony prywatności, a następnie kliknij **Kontynuuj**.
3. Zaznacz pole wyboru **Rozumiem** i kliknij **Aktualizuj**.
4. Zaznacz pole wyboru **Określ folder tymczasowy**.
5. Określ folder, do którego zostaną wyeksportowane dane wykazu.
   Dane generowane podczas eksportu zostają zaszyfrowane. Po zakończeniu migracji folder tymczasowy jest automatycznie usuwany.
6. Kliknij **Gotowe**.

Aby pominąć migrację danych wykazu

1. Na komputerze z zainstalowaną usługą wykazu uruchom program instalacyjny rozwiązania Acronis Cyber Protect.
2. Zaakceptuj warunki umowy licencyjnej i zasady ochrony prywatności, a następnie kliknij **Kontynuuj**.
3. Zaznacz pole wyboru **Rozumiem** i kliknij **Aktualizuj**.
4. Wyczyść pole wyboru **Określ folder tymczasowy**.
5. Kliknij **Gotowe**.
6. Potwierdź wybór.

W wyniku tych działań istniejące dane wykazu będą niedostępne po aktualizacji do rozwiązania Acronis Cyber Protect 15 Update 4. Aby odtworzyć dane wykazu, uruchom operację tworzenia kopii zapasowej.

Uwaga
Jeśli usługa wykazu, węzeł magazynowania i serwer zarządzania działają na różnych komputerach, koniecznie zaktualizuj je wszystkie do rozwiązania Acronis Cyber Protect 15 Update 4 w tej kolejności:

1. Serwer zarządzania
2. Węzeł magazynowania
3. Usługa wykazu

Dodawanie lokalizacji zarządzanej

Lokalizację zarządzaną można zorganizować:

- W folderze lokalnym:
  - Na dysku twardym lokalnym dla węzła magazynowania
  - W magazynie SAN widocznym dla systemu operacyjnego jako urządzenie podłączone lokalnie
- W folderze sieciowym:
  - W udziale SMB/CIFS
  - W magazynie SAN widocznym dla systemu operacyjnego jako folder sieciowy
  - W systemie NAS
- Na urządzeniu taśmowym podłączonym lokalnie do węzła magazynowania
  Lokalizacje oparte na taśmie są tworzone w postaci pul taśm. Domyślnie jest dostępna jedna pula taśm. W razie potrzeby możesz utworzyć inne pule taśm, zgodnie z opisem zamieszczonym w dalszej części tej sekcji.

Aby utworzyć lokalizację zarządzaną w folderze lokalnym lub sieciowym

1. Wykonaj jedną z następujących czynności:
   - Kliknij **Magazyn kopii zapasowych** > **Dodaj lokalizację**, a następnie kliknij **Węzeł magazynowania**.
   - W przypadku tworzenia planu ochrony kliknij **Miejsce docelowe kopii zapasowej** > **Dodaj lokalizację**, a następnie kliknij **Węzeł magazynowania**.
   - Kliknij **Ustawienia** > **Węzły magazynowania**, wybierz węzeł magazynowania, który będzie zarządzać lokalizacją, a następnie kliknij **Dodaj lokalizację**.
2. W polu **Nazwa** określ unikatową nazwę lokalizacji. „Unikatowa nazwa” oznacza, że nie może istnieć inna lokalizacja o tej samej nazwie zarządzana przez ten sam węzeł magazynowania.
3. [Opcjonalnie] Wybierz węzeł magazynowania, który będzie zarządzał lokalizacją. Jeśli w kroku 1 została wybrana ostatnia opcja, nie można zmienić węzła magazynowania.
4. Wybierz nazwę lub adres IP węzła magazynowania, których agent będzie używać w celu uzyskania dostępu do tej lokalizacji.
   Nazwa węzła magazynowania jest domyślnie wybrana. Jeśli serwer DNS nie może przypisać nazwy hosta do adresu IP, co skutkuje brakiem dostępu, trzeba zmienić to ustawienie. Aby

zmienić to ustawienie później, kliknij **Magazyn kopii zapasowych** > dana lokalizacja > **Edytuj**, a następnie zmień wartość pola **Adres**.

5. Wprowadź ścieżkę odpowiedniego folderu lub przejdź do niego.
6. Kliknij **Gotowe**. Oprogramowanie sprawdzi dostęp do określonego folderu.
7. [Opcjonalnie] Włącz deduplikację kopii zapasowej w tej lokalizacji.

   Deduplikacja minimalizuje ruch w sieci związany z tworzeniem kopii zapasowych oraz ogranicza rozmiar kopii zapasowych przechowywanych w danej lokalizacji przez eliminowanie duplikatów bloków dysków.

   Informacje na temat ograniczeń deduplikacji zawiera sekcja „Ograniczenia deduplikacji".
8. [Tylko w przypadku włączonej deduplikacji] Określ lub zmień wartość pola **Ścieżka bazy danych deduplikacji**.

   Musi to być folder na dysku twardym lokalnym dla węzła magazynowania. Aby zwiększyć wydajność systemu, zalecamy utworzenie bazy danych deduplikacji i lokalizacji zarządzanej na różnych dyskach.

   Aby uzyskać więcej informacji na temat bazy danych deduplikacji, zobacz „Sprawdzone praktyki dotyczące deduplikacji".
9. [Opcjonalnie] Określ, czy lokalizacja ma być chroniona za pomocą szyfrowania. Wszelkie dane zapisywane w tej lokalizacji będą szyfrowane, a wszelkie odczytywane dane będą deszyfrowane w sposób przezroczysty przez węzeł magazynowania przy użyciu odpowiadającego danej lokalizacji klucza szyfrowania przechowywanego na tym węźle.

   Więcej informacji o szyfrowaniu, zobacz „Szyfrowanie lokalizacji".
10. [Opcjonalnie] Określ, czy ma być tworzony wykaz kopii zapasowych przechowywanych w danej lokalizacji. Wykaz danych ułatwia znalezienie wymaganej wersji danych i wybranie jej do odzyskania.

    Jeśli na serwerze zarządzania zarejestrowano kilka usług katalogowania, wybierz usługę, która będzie katalogować kopie zapasowe przechowywane w danej lokalizacji.

    Katalogowanie można później włączyć lub wyłączyć, zgodnie z opisem podanym w sekcji „Jak włączyć lub wyłączyć katalogowanie".
11. Aby utworzyć lokalizację, kliknij **Gotowe**.

Aby utworzyć lokalizację zarządzaną na urządzeniu taśmowym

1. Kliknij **Magazyn kopii zapasowych** > **Dodaj lokalizację** albo podczas tworzenia planu ochrony kliknij **Miejsce docelowe kopii zapasowej** > **Dodaj lokalizację**.
2. Kliknij **Taśmy**.
3. [Opcjonalnie] Wybierz węzeł magazynowania, który będzie zarządzał lokalizacją.
4. Wykonaj czynności opisane w sekcji „Tworzenie puli", rozpoczynając od kroku 4.

Uwaga
Domyślnie w celu uzyskania dostępu do zarządzanej lokalizacji taśmowej agenty używają nazwy węzła magazynowania. Aby agenty używały adresu IP węzła magazynowania, kliknij **Magazyn kopii zapasowych** > dana lokalizacja > **Edytuj**, a następnie zmień wartość pola **Adres**.

Deduplication

Ograniczenia deduplikacji

Typowe ograniczenia

Zaszyfrowanych kopii zapasowych nie można deduplikować. Jeśli chcesz stosować zarówno deduplikację, jak i szyfrowanie, pozostaw kopie zapasowe niezaszyfrowane i skieruj je do lokalizacji, w której jest włączona obsługa obu tych funkcji.

Tworzenie kopii zapasowych na poziomie dysku

Deduplikacji bloków dysku nie można dokonać, jeśli rozmiar jednostki alokacji woluminu — nazywanej także rozmiarem klastra lub rozmiarem bloku — jest niepodzielny przez 4 KB.

Uwaga
W przypadku większości woluminów NTFS i ext3 jednostka alokacji ma rozmiar 4 KB. Umożliwia to deduplikację na poziomie bloków. Inne przykładowe rozmiary jednostki alokacji umożliwiające deduplikację na poziomie bloków to 8 KB, 16 KB oraz 64 KB.

Kopia zapasowa na poziomie plików

Zaszyfrowane pliki nie są deduplikowane.

Deduplikacja i strumienie danych NTFS

W systemie plików NTFS z plikiem można skojarzyć co najmniej jeden zestaw danych, nazywany często *alternatywnym strumieniem danych*.

Alternatywne strumienie danych takiego pliku są wraz z nim także umieszczane w kopii zapasowej. Jednak strumienie takie nigdy nie podlegają deduplikacji, nawet w przypadku deduplikacji samego pliku.

Sprawdzone praktyki dotyczące deduplikacji

Deduplikacja to złożony proces zależny od wielu czynników.

Najważniejsze czynniki mające wpływ na szybkość deduplikacji to:

- Szybkość dostępu do bazy danych deduplikacji
- Rozmiar pamięci RAM węzła magazynowania
- Liczba lokalizacji deduplikacji utworzonych w węźle magazynowania.

Aby zwiększyć wydajność deduplikacji, zastosuj poniższe zalecenia.

Umieść bazę danych deduplikacji i lokalizację deduplikacji na osobnych urządzeniach fizycznych

Baza danych deduplikacji przechowuje wartości skrótów wszystkich elementów przechowywanych w lokalizacji z wyjątkiem tych, które nie mogą być poddane deduplikacji, na przykład plików zaszyfrowanych.

Aby przyspieszyć dostęp do bazy danych deduplikacji, baza i lokalizacja muszą zostać umieszczone na osobnych urządzeniach fizycznych.

Najlepiej jest przydzielić lokalizacji i bazie danych specjalne urządzenia. Jeśli nie jest to możliwe, unikaj przynajmniej umieszczania lokalizacji lub bazy danych na wspólnym dysku z systemem operacyjnym. Jest to związane z dużą liczbą operacji odczytu/zapisu twardego dysku wykonywanych przez system operacyjny, co znacząco zwalnia deduplikację.

Wybór dysku dla bazy danych deduplikacji

- Baza danych musi znajdować się na dysku niewymiennym. Nie należy umieszczać bazy danych deduplikacji na zewnętrznych dyskach wymiennych.
- Aby maksymalnie skrócić czas dostępu do bazy danych, przechowuj ją bezpośrednio na podłączonym napędzie, a nie w zamontowanym woluminie sieciowym. Opóźnienie sieci można znacznie obniżać wydajność deduplikacji.
- Rozmiar miejsca na dysku wymaganego do poprawnego działania bazy danych deduplikacji można oszacować za pomocą następującego równania:

$$S = U * 90 / 65536 + 10$$

Znaczenie:

S — rozmiar dysku (w GB)

U — planowany rozmiar unikatowych danych w magazynie danych deduplikacji (w GB)

Jeśli na przykład planowany rozmiar unikatowych danych w magazynie danych deduplikacji wynosi U=5 TB, baza danych deduplikacji będzie wymagała co najmniej następującej ilości wolnego miejsca:

$$S = 5000 * 90 / 65536 + 10 = 17 \text{ GB}$$

Wybór dysku dla lokalizacji deduplikacji

Aby chronić dane przed utratą, najlepiej jest korzystać z macierzy RAID 10, 5 lub 6. Macierz RAID 0 nie jest zalecana, ponieważ nie jest odporna na awarie. Macierz RAID 1 nie jest zalecana z powodu względnie niewielkiej prędkości. Do tego zastosowania nadają się zarówno dyski lokalne, jak i SAN.

Od 40 do 160 MB pamięci RAM na 1 TB unikatowych danych

Po osiągnięciu limitu deduplikacja zostanie zatrzymana, ale tworzenie kopii zapasowych i odzyskiwanie nadal będzie działać. Zwiększenie pamięci RAM w węźle magazynowania spowoduje

wznowienie deduplikacji po utworzeniu następnej kopii zapasowej. Ogólnie mówiąc, im większa jest pamięć RAM, tym więcej unikatowych danych można przechowywać.

Tylko jedna lokalizacja deduplikacji na każdy węzeł magazynowania

Zdecydowanie zaleca się utworzenie w węźle magazynowania tylko jednej lokalizacji deduplikacji. W przeciwnym razie cała dostępna pamięć RAM może zostać proporcjonalnie rozdzielona między poszczególne lokalizacje.

Brak aplikacji rywalizujących o zasoby

Na komputerze z węzłem magazynowania nie powinny być uruchomione aplikacje o dużym zapotrzebowaniu na zasoby systemowe, takie jak systemy zarządzania bazami danych (DBMS) lub systemy planowania zasobów (ERP).

Procesor wielordzeniowy z częstotliwością taktowania wynoszącą co najmniej 2,5 GHz

Zalecamy użycie procesora mającego co najmniej cztery rdzenie i częstotliwość taktowania nie niższą niż 2,5 GHz.

Wystarczająca ilość wolnego miejsca w lokalizacji

Deduplikacja w lokalizacji docelowej wymaga tyle wolnego miejsca, ile zajmują dane kopii zapasowej bezpośrednio po jej zapisaniu w lokalizacji. Bez kompresji lub deduplikacji w miejscu źródłowym wartość ta jest równa rozmiarowi oryginalnych danych uwzględnionych w danej operacji tworzenia kopii zapasowej.

Szybka sieć lokalna

Zaleca się użycie sieci lokalnej 1 Gb. Pozwoli ona na równoległe wykonywanie 5-6 kopii zapasowych z deduplikacją bez wyraźnej redukcji szybkości.

Tworzenie kopii zapasowej typowego komputera przed utworzeniem kopii zapasowych kilku komputerów o podobnej zawartości

W przypadku tworzenia kopii zapasowych kilku komputerów o podobnej zawartości zaleca się najpierw utworzenie kopii zapasowej jednego komputera, a następnie odczekanie do zakończenia indeksowania danych uwzględnionych w kopii zapasowej. Po tym czasie tworzenie kopii zapasowych pozostałych komputerów będzie szybsze dzięki wydajnej deduplikacji. Z uwagi na zaindeksowanie kopii zapasowej pierwszego komputera większość danych znajduje się już w magazynie danych deduplikacji.

Tworzenie kopii zapasowych poszczególnych komputerów o różnych porach

Jeśli tworzysz kopie zapasowe dużej liczby komputerów, rozłóż w czasie operacje tworzenia kopii zapasowych. W tym celu utwórz kilka planów ochrony z różnymi harmonogramami.

Szyfrowanie lokalizacji

Jeśli chronisz lokalizację za pomocą szyfrowania, wszelkie dane zapisywane w tej lokalizacji będą szyfrowane, a wszelkie odczytywane dane będą deszyfrowane w sposób przezroczysty przez węzeł magazynowania przy użyciu odpowiadającego danej lokalizacji klucza szyfrowania przechowywanego na tym węźle. W przypadku kradzieży nośnika danych lub uzyskania do niego dostępu przez osobę nieuprawnioną odszyfrowanie przez nią zawartości lokalizacji bez dostępu do węzła magazynowania będzie niemożliwe.

To szyfrowanie nie ma nic wspólnego z szyfrowaniem kopii zapasowej określonym w planie ochrony i wykonywanym przez agenta. Jeśli kopia zapasowa jest już zaszyfrowana, szyfrowanie po stronie węzła magazynowania zostanie zastosowane po szyfrowaniu wykonanym przez agenta.

Aby chronić lokalizację za pomocą szyfrowania

1. Określ i potwierdź słowo (hasło), którego chcesz użyć do wygenerowania klucza szyfrowania.
   W słowie jest uwzględniana wielkość liter. Podczas podłączania lokalizacji do innego węzła magazynowania zostanie wyświetlona prośba o podanie tego słowa.
2. Wybierz jeden z następujących algorytmów szyfrowania:
   - **AES 128** — zawartość lokalizacji będzie szyfrowana przy użyciu algorytmu Advanced Encryption Standard (AES) z kluczem 128-bitowym.
   - **AES 192** — zawartość lokalizacji będzie szyfrowana przy użyciu algorytmu AES z kluczem 192-bitowym.
   - **AES 256** — zawartość lokalizacji będzie szyfrowana przy użyciu algorytmu AES z kluczem 256-bitowym.
3. Kliknij **OK**.

Algorytm kryptograficzny AES działa w trybie wiązania bloków szyfrogramu (Cipher-Block Chaining — CBC) i korzysta z losowo wygenerowanego klucza o długości zdefiniowanej przez użytkownika: 128, 192 lub 256 bitów. Im większy rozmiar klucza, tym dłużej trwa szyfrowanie przez program kopii zapasowych przechowywanych w lokalizacji i tym lepiej są one zabezpieczone.

Klucz szyfrowania jest następnie szyfrowany metodą AES-256, w której jako klucz służy skrót SHA-256 wybranego słowa. Samo słowo nie jest przechowywane w żadnym miejscu na dysku — do celów weryfikacji służy skrót słowa. Dzięki tym dwupoziomowym zabezpieczeniom kopie zapasowe są chronione przed nieautoryzowanym dostępem, ale odzyskanie utraconego słowa jest niemożliwe.

Katalogowanie

Wykaz danych

Wykaz danych ułatwia znalezienie wymaganej wersji danych i wybranie jej do odzyskania. W wykazie danych pokazywane są dane zapisane we wszystkich lokalizacjach zarządzanych objętych katalogowaniem.

Sekcja **Wykaz** jest wyświetlana na karcie **Magazyn kopii zapasowych** tylko wtedy, gdy na serwerze zarządzania jest zarejestrowana co najmniej jedna usługa wykazu. Aby uzyskać informacje na temat instalowania usługi wykazu, zobacz „Instalowanie węzła magazynowania i usługi wykazu”.

Sekcja **Wykaz** jest widoczna tylko dla administratorów organizacji.

Ograniczenia

Katalogowanie jest obsługiwane tylko w przypadku kopii zapasowych na poziomie dysku i plików komputerów fizycznych oraz kopii zapasowych maszyn wirtualnych.

Następujące dane nie mogą być wyświetlane w wykazie:

- Dane z zaszyfrowanych kopii zapasowych
- Dane uwzględnione w kopii zapasowej na urządzeniach taśmowych
- Dane uwzględnione w kopii zapasowej w magazynie chmurowym
- Dane uwzględnione w kopii zapasowej przez program Acronis Cyber Protect w wersji starszej niż 12.5

Wybór danych do odzyskania z kopii zapasowej

1. Kliknij **Magazyn kopii zapasowych** > **Wykaz**.
2. Jeśli na serwerze zarządzania zarejestrowano kilka usług katalogowania, wybierz usługę, która kataloguje kopie zapasowe przechowywane w danej lokalizacji.

   Uwaga
   Aby sprawdzić, która usługa kataloguje lokalizację, wybierz lokalizację w obszarze **Magazyn kopii zapasowych** > **Lokalizacje** > **Lokalizacje**, a następnie kliknij **Szczegóły**.

3. Oprogramowanie wyświetli wszystkie komputery uwzględnione w kopiach zapasowych umieszczonych w lokalizacjach zarządzanych katalogowanych przez wybraną usługę wykazu. Wybierz dane do odzyskania, przeglądając foldery lub korzystając z funkcji wyszukiwania.
   - **Przeglądanie**
     Kliknij dwukrotnie komputer, aby wyświetlić dyski, woluminy, foldery i pliki uwzględnione w kopii zapasowej.
     Aby odzyskać dysk, wybierz dysk oznaczony następującą ikoną: 
     Aby odzyskać wolumin, kliknij dwukrotnie zawierający go dysk, a następnie wybierz wolumin.
     Aby odzyskać pliki i foldery, przejrzyj wolumin, w którym się one znajdują. Można przeglądać woluminy oznaczone ikoną folderu: 
   - **Wyszukiwanie**
     W polu wyszukiwania wpisz informacje pomocne w identyfikacji wymaganych elementów danych (może to być nazwa komputera, pliku lub folderu bądź etykieta dysku), a następnie kliknij **Szukaj**.

Można używać gwiazdki (*) i znaku zapytania (?) jako symboli wieloznacznych.

W wyniku wyszukiwania zostanie wyświetlona lista elementów danych z kopii zapasowej, których nazwy całkowicie lub częściowo pasują do wprowadzonej wartości.

4. Domyślnie dane są przywracane do ostatniego możliwego punktu w czasie. W przypadku wybrania jednego elementu można wybrać punkt odzyskiwania za pomocą przycisku **Wersje**.
5. Po wybraniu wymaganych danych wykonaj jedną z następujących czynności:
   - Kliknij **Odzyskaj**, a następnie skonfiguruj parametry operacji odzyskiwania zgodnie z opisem w „Odzyskiwanie”.
   - [Tylko w przypadku plików/folderów] Jeśli chcesz zapisać pliki jako plik .zip, kliknij **Pobierz**, wybierz lokalizację, w której mają zostać zapisane dane, a następnie kliknij **Zapisz**.

Sprawdzone praktyki dotyczące katalogowania

Aby zwiększyć wydajność katalogowania, postępuj zgodnie z poniższymi zaleceniami.

Instalacja

Zalecamy zainstalowanie usługi wykazu i węzła magazynowania na oddzielnych komputerach. W przeciwnym razie te komponenty będą konkurować o zasoby procesora i pamięci RAM.

Jeśli na serwerze zarządzania zostało zarejestrowanych kilka węzłów magazynowania, jedna usługa wykazu wystarczy, chyba że pogorszy się wydajność indeksowania lub wyszukiwania. Jeśli na przykład zauważysz, że katalogowanie działa 24/7 (czyli, że nie ma przerw w katalogowaniu), zainstaluj jeszcze jedną usługę wykazu na oddzielnym komputerze. Następnie usuń niektóre z lokalizacji zarządzanych i odtwórz je za pomocą nowej usługi wykazu. Kopie zapasowe zapisane w tych lokalizacjach nie zostaną naruszone.

Wymagania systemowe

Parametr	Wartość minimalna	Wartość zalecana
Liczba rdzeni procesora	2	4 i więcej
Pamięć RAM	8 GB	16 GB i więcej
Dysk twardy	Napęd dysku twardego 7200 obr./min	Dysk SSD
Połączenie sieciowe między komputerem z węzłem magazynowania i a komputerem z usługą wykazu	100 Mb/s	1 Gb/s

Jak włączyć lub wyłączyć katalogowanie

Jeśli jest włączone katalogowanie dla lokalizacji zarządzanej, zawartość każdej nowo utworzonej kopii zapasowej kierowanej do tej lokalizacji jest niezwłocznie dodawana do wykazu danych.

Katalogowanie można włączyć podczas dodawania lokalizacji zarządzanej lub później. W katalogowanie jest włączone, wszystkie kopie zapasowe, które są przechowywane w danej lokalizacji, a nie zostały wcześniej skatalogowane, zostaną skatalogowane po utworzeniu następnej kopii zapasowej w tej lokalizacji.

Proces katalogowania może trochę potrwać, zwłaszcza gdy w danej lokalizacji są tworzone kopie zapasowe wielu komputerów. Katalogowanie można w każdej chwili wyłączyć. Kopie zapasowe utworzone przed wyłączeniem zostaną skatalogowane. Nowo utworzone kopie zapasowe już nie będą katalogowane.

Aby skonfigurować katalogowanie dla już istniejącej lokalizacji

1. Kliknij **Magazyn kopii zapasowych** > **Lokalizacje**.
2. Kliknij **Lokalizacje** i wybierz lokalizację zarządzaną, dla której chcesz skonfigurować katalogowanie.
3. Kliknij **Edytuj**.
4. Aktywuj lub dezaktywuj przełącznik **Usługa wykazu**.
5. Kliknij **Gotowe**.

Ustawienia systemu

Ustawienia te są dostępne tylko w ramach wdrożeń lokalnych.

Aby uzyskać dostęp do tych ustawień, kliknij **Ustawienia** > **Ustawienia systemowe**.

Sekcja **Ustawienia systemowe** jest widoczna tylko dla administratorów organizacji.

Powiadomienia e-mail

Istnieje możliwość skonfigurowania ustawień globalnych wspólnych dla wszystkich powiadomień e-mail wysyłanych z serwera zarządzania.

W domyślnych opcjach tworzenia kopii zapasowej możesz zastąpić te ustawienia wyłącznie dla zdarzeń występujących podczas tworzenia kopii zapasowej. W takim przypadku ustawienia globalne będą stosowane do operacji innych niż tworzenie kopii zapasowych.

W przypadku tworzenia planu ochrony możesz wybrać używane ustawienia: ustawienia globalne lub ustawienia określone w domyślnych opcjach tworzenia kopii zapasowych. Możesz też je zastąpić wartościami niestandardowymi stosowanymi tylko w odniesieniu do tego planu.

Ważne
Zmiana globalnych ustawień powiadomień e-mail wpłynie na wszystkie korzystające z nich plany ochrony.

Zanim skonfigurujesz te ustawienia upewnij się, że zostały skonfigurowane ustawienia **serwera poczty e-mail**.

Aby skonfigurować globalne 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. [Opcjonalnie] W polu **Temat** zmień temat powiadomienia pocztą e-mail.
   Możesz użyć następujących zmiennych:
   - `[Alert]` — podsumowanie alertu.
   - `[Urządzenie]` — nazwa urządzenia.
   - `[Plan]` — nazwa planu, który wygenerował alert.
   - `[Serwer zarządzania]` — nazwa hosta komputera, na którym jest zainstalowany serwer zarządzania.
   - `[Jednostka]` — nazwa jednostki, do której należy komputer.

   Domyślnym tematem jest `[Alert]` **Urządzenie:** `[Urządzenie]` **Plan:** `[Plan]`
4. [Opcjonalnie] Zaznacz pole wyboru **Codziennie zestawienie aktywnych alertów**, a następnie wykonaj następujące czynności:

a. Określ godzinę, kiedy zestawienie będzie wysyłane.

b. [Opcjonalnie] Zaznacz pole wyboru **Nie wysyłaj komunikatów „Brak aktywnych alertów"**.

5. [Opcjonalnie] Wybierz język, który będzie używany w powiadomieniach e-mail.
6. Zaznacz pola wyboru odpowiadające zdarzeniom, o których chcesz otrzymywać powiadomienia. Możesz wybrać z listy wszystkich możliwych alertów zgrupowanych według wagi.
7. Kliknij **Zapisz**.

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**
   - **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.
4. [Tylko w przypadku usług Gmail, Yahoo Mail i Outlook.com] Określ poświadczenia konta, które będzie używane do wysyłania wiadomości.
5. [Tylko dla niestandardowej usługi e-mail] 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.

Zabezpieczenia

Za pomocą tych opcji możesz wzmocnić zabezpieczenia lokalnego wdrożenia programu Acronis Cyber Protect.

Wylogowuj nieaktywnych użytkowników po

Ta opcja umożliwia określenie limitu czasu funkcji automatycznego wylogowywania użytkownika z powodu jego braku aktywności. Gdy do wyczerpania limitu czasu zostaje jedna minuta, program monituje użytkownika, by pozostał zalogowany. W razie dalszego braku aktywności użytkownik zostanie wylogowany, a wszystkie jego niezapisane zmiany zostaną utracone.

Ustawienie wstępne: **Włączono. Limit czasu: 10 minut.**

Pokaż powiadomienie o ostatnim zalogowaniu bieżącego użytkownika

Ta opcja umożliwia wyświetlenie daty i godziny ostatniego udanego zalogowania się użytkownika, liczby błędów uwierzytelniania od tego czasu oraz adresu IP użytego podczas ostatniej udanej operacji logowania. Informacje te są wyświetlane u dołu ekranu podczas każdego logowania się użytkownika.

Ustawienie wstępne: **Wyłączono**.

Ostrzegaj o wygaśnięciu hasła lokalnego lub domenowego

Ta opcja umożliwia włączenie wyświetlania terminu wygaśnięcia hasła dostępu użytkownika do serwera Acronis Cyber Protect Management Server. Jest to hasło lokalne lub domenowe, za pomocą którego użytkownik loguje się na komputerze z zainstalowanym serwerem zarządzania. Czas pozostały do wygaśnięcia hasła jest wyświetlany u dołu ekranu oraz w menu konta w prawym górnym rogu.

Ustawienie wstępne: **Wyłączono**.

Aktualizacje

Ta opcja umożliwia określenie, czy program Acronis Cyber Protect ma sprawdzać dostępność nowej wersji po każdym zalogowaniu się administratora organizacji w konsoli internetowej Cyber Protect.

Ustawienie wstępne: **Włączono**.

Jeśli ta opcja jest wyłączona, administrator może sprawdzić dostępność aktualizacji ręcznie zgodnie z opisem zamieszczonym w sekcji „Sprawdzanie dostępności aktualizacji”.

Domyślne opcje tworzenia kopii zapasowej

Wartości domyślne opcji tworzenia kopii zapasowej są wspólne dla wszystkich planów ochrony na danym serwerze zarządzania. Administrator organizacji może zmienić domyślną wartość opcji na inną niż predefiniowana. Nowa wartość będzie domyślnie używana we wszystkich planach ochrony utworzonych po wprowadzeniu zmiany.

Podczas tworzenia planu ochrony użytkownik może zastąpić wartość domyślną wartością niestandardową, która będzie używana tylko w ramach tego planu.

Aby zmienić domyślną wartość opcji

1. Zaloguj się do konsoli internetowej Cyber Protect jako administrator organizacji.
2. Kliknij **Ustawienia** > **Ustawienia systemowe**.
3. Rozwiń sekcję **Domyślne opcje tworzenia kopii zapasowych**.
4. Wybierz opcję, a następnie wprowadź wymagane zmiany.
5. Kliknij **Zapisz**.

Ustawienia ochrony

Aby skonfigurować ustawienia ochrony, w konsoli internetowej Cyber Protect przejdź do sekcji **Ustawienia** > **Ochrona**.

Więcej informacji na temat konkretnych ustawień i procedur można znaleźć w odpowiednim temacie w tej sekcji.

Aktualizowanie definicji ochrony

Domyślnie wszystkie agenty ochrony mogą się łączyć z Internetem i pobierać aktualizacje następujących komponentów:

- Ochrona antywirusowa
- Ocena luk w zabezpieczeniach
- Zarządzanie poprawkami

Agenty z rolą Aktualizator

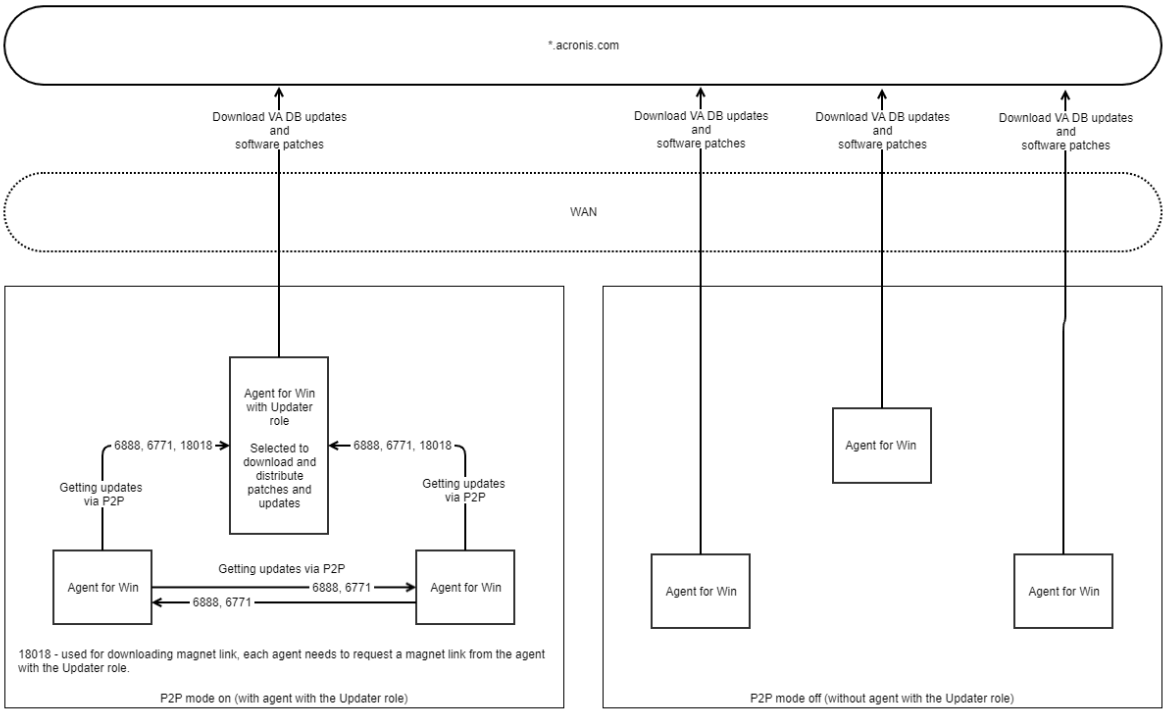
Administrator może zminimalizować ruch na łączu sieciowym, wybierając w środowisku co najmniej jednego agenta ochrony i przypisując mu rolę Aktualizator. W związku z tym tylko tak wyznaczone agenty będą się łączyć z Internetem i pobierać aktualizacje. Pozostałe agenty będą się łączyć z tymi wyznaczonymi agentami aktualizującymi przy użyciu technologii peer-to-peer i od nich pobierać aktualizacje.

Agenty, które nie mają przypisanej roli Aktualizator, będą się łączyć z Internetem, jeśli w środowisku nie będzie wyznaczonego agenta-aktualizatora lub jeśli przez około 5 minut nie uda się nawiązać połączenia z wyznaczonym agentem-aktualizatorem.

Zanim przypiszesz agentowi rolę Aktualizator, dopilnuj, aby komputer, na którym działa dany agent, był wystarczająco wydajny, miał stabilne, szybkie połączenie z Internetem oraz wystarczającą ilość miejsca na dysku.

Rolę Aktualizator można przypisać do wielu agentów w środowisku. Dzięki temu w sytuacji, gdy agent mający przypisaną rolę Aktualizator jest offline, inne agenty z tą rolą mogą służyć jako źródła zaktualizowanych definicji ochrony.

Poniższy diagram ilustruje dostępne opcje na pobranie aktualizacji ochrony. Po lewej stronie znajduje się agent przypisany do roli aktualizatora. Ten agent łączy się z Internetem, aby pobrać aktualizacje ochrony, a agenty równorzędne łączą się z aktualizatorem, aby pobrać najnowsze aktualizacje. Po prawej stronie żaden agent nie jest przypisany do roli aktualizatora, więc wszyscy agenci łączą się z Internetem, aby pobrać aktualizacje ochrony.



Aby przygotować komputer do roli Aktualizator

1. Na komputerze, na którym będzie działać agent z rolą Aktualizator, zastosuj następujące reguły zapory:
   - Ruch przychodzący „updater_incoming_tcp_ports”: zezwól na połączenia przy użyciu portów TCP 18018 i 6888 dla wszystkich profili zapory (publicznego, prywatnego i domeny).
   - Ruch przychodzący „updater_incoming_udp_ports”: zezwól na połączenia przy użyciu portu UDP 6888 dla wszystkich profili zapory (publicznego, prywatnego i domeny).
2. Uruchom ponownie usługę Acronis Agent Core Service.
3. Uruchom ponownie usługę zapory.

Jeśli te reguły nie zostaną zastosowane, a zapora jest włączona, inne agenty będą pobierać aktualizacje z chmury.

Aby przypisać rolę aktualizatora do agenta

1. W konsoli internetowej Cyber Protect przejdź do sekcji **Ustawienia** > **Agenci**.
2. Wybierz komputer z agentem, do którego chcesz przypisać rolę aktualizatora.
3. Kliknij **Szczegóły** i włącz przełącznik **Użyj tego agenta, aby pobrać oraz rozpowszechnić poprawki i aktualizacje**.

Planowanie aktualizacji

Można zaplanować automatyczne aktualizacje definicji ochrony we wszystkich agentach lub aktualizować je ręcznie w wybranych agentach.

Aby zaplanować aktualizacje automatyczne

1. W konsoli internetowej Cyber Protect przejdź do sekcji **Ustawienia** > **Ochrona** > **Aktualizacja definicji ochrony**.
2. Wybierz **Harmonogram**.
3. W polu **Typ harmonogramu** wybierz jedną z następujących opcji:
   - **Codziennie**

     Wybierz dni tygodnia, w które mają być aktualizowane definicje ochrony.

     W polu **Rozpocznij o** wybierz godzinę rozpoczynania aktualizacji.
   - **Co godzinę**

     Ustaw dokładny harmonogram aktualizacji.

     W polu **Uruchamiaj co** ustaw częstość aktualizacji.

     W polach **Od** ... **Do** określ zakres czasu, w którym mają być dokonywane aktualizacje.

Aby ręcznie zaktualizować definicje ochrony

1. W konsoli internetowej Cyber Protect przejdź do sekcji **Ustawienia** > **Agenci**.
2. Wybierz komputery, na których chcesz zaktualizować definicje ochrony agentów, i kliknij **Aktualizuj definicje**.

Zmienianie lokalizacji pobieranych plików

Definicje ochrony są pobierane do domyślnego folderu tymczasowego na komputerze, a następnie zapisywane w folderze programu Acronis.

Aby zmienić folder tymczasowy używany podczas pobierania

1. Na komputerze z serwerem zarządzania otwórz plik `atp-database-mirror.json` do edycji.

   Plik ten można znaleźć w następującej lokalizacji:
   - W systemie Windows: `%programdata%\Acronis\AtpDatabaseMirror\`
   - W systemie Linux: `/var/lib/Acronis/AtpDatabaseMirror/`
2. Zmień wartość parametru `"enable_user_config"` na `true`.

```
{
"sysconfig":
{
...
"enable_user_config": true
}
```

```
...
}
```

3. Na komputerze z serwerem zarządzania otwórz plik `config.json` do edycji.
   Plik ten można znaleźć w następującej lokalizacji:
   - W systemie Windows: `%programdata%\Acronis\AtpDatabaseMirror\`
   - W systemie Linux: `/var/lib/Acronis/AtpDatabaseMirror/`
4. Dodaj następujący wiersz: `"mirror_temp_dir": "<ścieżka_do_nowej_lokalizacji_pobieranych_plików>"`
   Na przykład:
   ```
   {
           "mirror_temp_dir": "C:\\temp"
   }
   ```
   Można podać ścieżkę bezwzględną lub względną w stosunku do folderu `AppData`.
   Jeśli nie można utworzyć folderu lub serwer zarządzania nie może w nim zapisywać, zostanie użyta lokalizacja domyślna.

Opcje zapisywania w pamięci podręcznej

Dane zapisywane w pamięci podręcznej znajdują się w następującej lokalizacji:

- Windows: `C:\ProgramData\Acronis\Agent\var\atp-downloader\Cache`
- W systemie Linux: `/opt/acronis/var/atp-downloader/Cache`
- W systemie macOS: `/Library/Application Support/Acronis/Agent/var/atp-downloader/Cache`

Można skonfigurować harmonogram czyszczenia nieaktualnych danych z pamięci podręcznej i ustawić limit jej rozmiaru. Można ustawić inne limity w przypadku komputerów z agentami, które nie są aktualizatorami, a inne w przypadku komputerów z agentami, które są aktualizatorami.

Źródło najnowszych definicji ochrony

Najnowsze definicje ochrony można pobierać z następujących lokalizacji:

- **Cloud**
  Agenty ochrony łączą się z Internetem i pobierają najnowsze definicje ochrony z magazynu Acronis Cloud. Domyślnie aktualizacje są sprawdzane i rozpowszechniane przez wszystkie agenty zarejestrowane na serwerze zarządzania. Więcej informacji na temat agentów z rolą Aktualizator można znaleźć w sekcji "Aktualizowanie definicji ochrony" (s. 658).
- **Cyber Protect Management Server**
  W przypadku wybrania tej opcji agenty nie potrzebują dostępu do Internetu. Łączą się tylko z serwerem zarządzania, na którym są przechowywane definicje ochrony. Jednak serwer zarządzania musi mieć połączenie z Internetem w celu pobrania najnowszych definicji ochrony.

- **Niestandardowe serwery internetowe**
  Ta opcja jest przeznaczona wyłącznie do rozwiązywania problemów i testowania oraz do stosowania w przypadku odseparowanych środowisk. Więcej informacji można znaleźć w sekcji "Aktualizowanie definicji ochrony w odseparowanym środowisku" (s. 662). Zazwyczaj należy ją zaznaczyć wyłącznie na prośbę zespołu pomocy technicznej firmy Acronis.

Połączenie zdalne

Gdy włączysz połączenie zdalne, w menu z prawej strony obszaru **Pulpit ochrony cybernetycznej** w konsoli internetowej Cyber Protect pojawią się opcje **Połącz przez klienta RDP** i **Połącz przez klienta HTML5**. Po wybraniu obciążenia na karcie **Urządzenia** zostanie otwarte menu z prawej strony.

Włączenie lub wyłączenie połączenia zdalnego ma wpływ na wszystkich użytkowników z organizacji.

Aby włączyć połączenie zdalne

1. W konsoli internetowej Cyber Protect przejdź do sekcji **Ustawienia** > **Ochrona**.
2. Kliknij **Połączenie zdalne**, a następnie włącz przełącznik **Podłączanie pulpitu zdalnego**.

Można też włączyć udostępnianie połączenia zdalnego. Wybierając tę opcję, można wygenerować łącze umożliwiające uzyskanie zdalnego dostępu do obciążenia. Takie łącze można udostępnić innym użytkownikom.

Aby włączyć udostępnianie połączenia zdalnego

1. W konsoli internetowej Cyber Protect przejdź do sekcji **Ustawienia** > **Ochrona**.
2. Zaznacz pole wyboru **Udostępnij połączenie pulpitu zdalnego**.

W wyniku tych działań w menu z prawej strony obszaru **Pulpit ochrony cybernetycznej** w konsoli internetowej Cyber Protect pojawi się opcja **Udostępnij połączenie zdalne**.

Aktualizowanie definicji ochrony w odseparowanym środowisku

Program Acronis Cyber Protect obsługuje aktualizowanie definicji ochrony w odseparowanym środowisku.

Aby zaktualizować definicje ochrony w odseparowanym środowisku

1. Poza odseparowanym środowiskiem zainstaluj drugi serwer zarządzania, który ma dostęp do Internetu.
   Dodatkowe informacje na ten temat można znaleźć w sekcji "Instalowanie serwera zarządzania" (s. 87).
2. Skopiuj definicje ochrony z serwera zarządzania online na dysk wymienny, a następnie przenieś je na serwer HTTP w odseparowanym środowisku.

Dodatkowe informacje na temat tego kroku można znaleźć w sekcjach "Pobieranie definicji na serwer zarządzania online" (s. 663) i "Przenoszenie definicji na serwer HTTP" (s. 664).

3. Na odseparowanym serwerze zarządzania skonfiguruj serwer HTTP jako źródło zaktualizowanych definicji ochrony.

   Dodatkowe informacje na temat tego kroku można znaleźć w sekcji "Konfigurowanie źródła definicji na odseparowanym serwerze zarządzania" (s. 665).

Pobieranie definicji na serwer zarządzania online

Po zainstalowaniu drugiego serwera zarządzania, który ma dostęp do Internetu, pobierz najnowsze definicje ochrony i skopiuj je na dysk wymienny, na przykład pamięć flash USB lub zewnętrzny dysk twardy.

Aby pobrać i skopiować definicje ochrony

1. Na komputerze z serwerem zarządzania online skopiuj folder `AtpDatabaseMirror` do wybranej lokalizacji, na przykład na pulpit lub do folderu `Temp`.

   Folder `AtpDatabaseMirror` znajduje się w następującej lokalizacji:

   - W systemie Windows: `%ProgramData%\Acronis\`
   - W systemie Linux: `/usr/lib/Acronis/`

2. Otwórz plik `atp_database_mirror.json` do edycji. Plik ten znajduje się w następującej lokalizacji:

   - W systemie Windows: `%Program Files%\Acronis\AtpDatabaseMirror`

     Uwaga
     W systemie Windows folder ten nie jest tym samym folderem, o którym była mowa w poprzednim kroku.

   - W systemie Linux: `/usr/lib/Acronis/AppDatabaseMonitor`

3. Edytuj plik `atp_database_mirror.json` następująco:

   a. Zmień wartość parametru `"enable_appdata_as_root"` na `false`.

   b. Zmień wartości wszystkich wpisów `"local_path"` na ścieżkę bezwzględną lokalizacji, w której mają zostać zapisane definicje ochrony.

4. Zapisz zmiany dokonane w pliku `atp_database_mirror.json`.

5. Na komputerze z serwerem zarządzania online zatrzymaj usługę **Acronis Management Server** przy użyciu następującego polecenia:

   - W systemie Windows (wiersz polecenia):

     ```
     sc stop AcrMngSrv
     ```

   - W systemie Linux (terminal):

     ```
     sudo systemctl stop acronis_ams.service
     ```

6. W folderze `AtpDatabaseMirror` skopiowanym do wybranej lokalizacji uruchom narzędzie `AtpDatabaseMirror` przy użyciu następującego polecenia:
   - W systemie Windows (wiersz polecenia):
     ```
     atp_database_mirror.exe -config atp_database_mirror.json
     ```
   - W systemie Linux (terminal):
     ```
     sudo ./atp_database_mirror -config atp_database_mirror.json
     ```

   Gdy wszystkie aktualizacje zostaną pobrane do folderu wskazanego w wierszu `"local_path"`, w oknie wiersza polecenia lub terminalu zostanie wyświetlony następujący wiersz:
   ```
   standing by for 1m0s
   ```
7. Zatrzymaj narzędzie `AtpDatabaseMirror`, naciskając klawisze CTRL+C.
8. Skopiuj pliki z folderu wskazanego w wierszu `"local_path"` na dysk wymienny.

Następnie trzeba skopiować pliki z dysku wymiennego na serwer HTTP w odseparowanym środowisku. W roli serwera HTTP można wykorzystać odseparowany serwer zarządzania. Więcej informacji można znaleźć w sekcji "Przenoszenie definicji na serwer HTTP" (s. 664).

Przenoszenie definicji na serwer HTTP

Do dystrybucji definicji ochrony w odseparowanym środowisku jest potrzebny specjalny serwer HTTP. W roli serwera HTTP można wykorzystać odseparowany serwer zarządzania.

Aby przenieść definicje ochrony na serwer HTTP

1. Na komputerze, na którym będzie działać serwer HTTP, skopiuj definicje ochrony do wybranego przez siebie folderu.
2. Uruchom serwer HTTP z poziomu folderu, do którego skopiowano definicje ochrony.
   Na przykład skorzystaj z języka Python i uruchom następujące polecenie:
   ```
   python -m http.server 8080
   ```

   Uwaga
   Możesz użyć dowolnego preferowanego serwera HTTP.
3. W folderze, do którego skopiowano definicje ochrony, otwórz do edycji następujące pliki `update-index.json`:
   - `./ngmp/update-index.json`
   - `./vapm/update-index.json`
4. W obu plikach `update-index.json` edytuj wszystkie pola `products > os > arch > components > versions > url` w sposób następujący:

a. Jako wartości `IP` i `port` podaj adres IP i port serwera HTTP.

b. Nie zmieniaj pozostałej części ścieżki.

Na przykład `"url": "http://192.168.1.10:8080/ngmp/win64/ngmp.zip"`, gdzie 192.168.1.10 jest adresem IP, a 8080 portem serwera HTTP. Część `/ngmp/win64/ngmp.zip` pozostaw bez zmian.

5. Zapisz zmiany wprowadzone w obu plikach `update-index.json`.

Następnie musisz skonfigurować źródło definicji ochrony na odseparowanym serwerze zarządzania. Więcej informacji można znaleźć w sekcji "Konfigurowanie źródła definicji na odseparowanym serwerze zarządzania" (s. 665).

Konfigurowanie źródła definicji na odseparowanym serwerze zarządzania

Po skonfigurowaniu serwera HTTP trzeba go skonfigurować na odseparowanym serwerze zarządzania jako źródło definicji ochrony.

Aby skonfigurować źródło definicji ochrony na odseparowanym serwerze zarządzania

1. W konsoli internetowej Cyber Protect odseparowanego serwera zarządzania przejdź do sekcji **Ustawienia** > **Ochrona** > **Aktualizacja definicji ochrony**.
2. Wybierz **Definicje**.
3. Wybierz **Niestandardowe** i podaj następujące ścieżki:

- W sekcji **Definicje do ochrony przed wirusami i złośliwym oprogramowaniem**:
  `http://<IP address of your HTTP server>:8080/scanner`
- W sekcji **Zaawansowane definicje do wykrywania**:
  `http://<IP address of your HTTP server>:8080/ngmp`
- W sekcji **Definicje do oceny luk w zabezpieczeniach i zarządzania poprawkami**:
  `http://<IP address of your HTTP server>:8080/vapm`

W wyniku tych działań agenty w odseparowanym środowisku pobiorą definicje ochrony z Twojego serwera HTTP.

Administrowanie kontami użytkowników i jednostkami organizacyjnymi

Wdrożenie lokalne

Funkcja opisana w tej sekcji jest dostępna tylko dla administratorów organizacji.

Aby uzyskać dostęp do tych ustawień, kliknij kolejno **Ustawienia** > **Konta**.

Jednostki i konta administracyjne

Aby zarządzać jednostkami i kontami administracyjnymi, w konsoli internetowej Cyber Protect przejdź do sekcji **Ustawienia** > **Konta**. Panel **Konta** zawiera grupę **Organizacja** wraz z drzewem jednostek (jeśli istnieje) oraz listę kont administracyjnych na wybranym poziomie hierarchii.

Jednostki

Grupa **Organizacja** jest tworzona automatycznie podczas instalacji serwera zarządzania. Licencja wersji Acronis Cyber Protect Advanced pozwala tworzyć grupy podrzędne nazywane jednostkami, które zwykle odpowiadają jednostkom organizacyjnym lub działom organizacji, i dodawać do nich konta administracyjne. W ten sposób możesz przekazać zarządzanie ochroną innym osobom, których uprawnienia dostępu będą ściśle ograniczone do odpowiednich jednostek. Informacje na temat tworzenia jednostki można znaleźć w sekcji "Tworzenie jednostek" (s. 671).

Każda jednostka może mieć jednostki dziecięce. Konta administracyjne jednostki nadrzędnej mają takie same prawa we wszystkich jej jednostkach podrzędnych. Grupa **Organizacja** jest jednostką nadrzędną najwyższego poziomu, więc konta administracyjne na tym poziomie mają takie same prawa we wszystkich jednostkach.

Konta administracyjne

Kontem administracyjnym jest każde konto umożliwiające zalogowanie się w konsoli internetowej Cyber Protect.

W konsoli internetowej Cyber Protect każde konto administracyjne ma uprawnienia do przeglądania wszystkich elementów znajdujących się na poziomie lub poniżej poziomu hierarchii jego jednostki albo do zarządzania nimi. Na przykład konto administracyjne w *organizacji* ma dostęp do tego najwyższego poziomu, a w związku z tym również dostęp do wszystkich jednostek tej organizacji, podczas gdy konto administracyjne w określonej *jednostce* ma dostęp tylko do tej jednostki i jej jednostek podrzędnych.

Które konta mogą być kontami administracyjnymi?

Jeśli serwer zarządzania jest zainstalowany na komputerze z systemem Windows, który należy do domeny Active Directory, prawa administracyjne można przyznać użytkownikom lokalnym albo

użytkownikom i grupom użytkowników w ramach danego lasu domeny Active Directory.

Domyślnie serwer zarządzania nawiązuje połączenie z kontrolerem domeny Active Directory chronione przy użyciu protokołu SSL/TLS. Jeśli nie jest to możliwe, nie zostanie nawiązane żadne połączenie. Można jednak zezwolić na połączenia niezabezpieczone — w tym celu należy edytować plik `auth-connector.json5`.

Aby korzystać z połączenia zabezpieczonego, upewnij się, że dla usługi Active Directory skonfigurowano protokół LDAP over SSL (LDAPS).

Aby skonfigurować protokół LDAPS dla usługi Active Directory

1. Na kontrolerze domeny utwórz i zainstaluj certyfikat LDAPS, który spełnia wymagania firmy Microsoft.

   Dodatkowe informacje o tym, jak to zrobić, można znaleźć w sekcji Enable LDAP over SSL with a third-party certification authority (Włączanie protokołu LDAP over SSL przy użyciu zewnętrznego urzędu certyfikacji) w dokumentacji firmy Microsoft.
2. Na kontrolerze domeny otwórz narzędzie **Microsoft Management Console** i sprawdź, czy w sekcji **Certyfikaty (Komputer lokalny)** > **Osobiste** > **Certyfikaty** jest dostępny certyfikat.
3. Uruchom ponownie kontroler domeny.
4. Sprawdź, czy jest włączony protokół LDAPS.

Aby zezwolić na niezabezpieczone połączenia z kontrolerem domeny

1. Zaloguj się na komputerze z zainstalowanym serwerem zarządzania.
2. Otwórz plik `auth-connector.json5` do edycji.

   Plik `auth-connector.json5` znajduje się w folderze `%APPDATA%\Acronis\AuthConnector`.
3. Przejdź do sekcji **sync** i w każdym wierszu **"connectionMode"** zastąp wartość **"ssl_only"** wartością **"auto"**.

   W trybie **auto** w przypadku braku możliwości nawiązania połączenia TLS nawiązywane jest połączenie niezabezpieczone.
4. Uruchom ponownie usługę **Acronis Service Manager Service** zgodnie z opisem podanym w sekcji "Aby uruchomić ponownie usługę Acronis Service Manager Service" (s. 204).

Uwaga
Jeśli serwer zarządzania nie należy do domeny Active Directory lub jest zainstalowany na komputerze z systemem Linux, prawa administracyjne można przyznać tylko użytkownikom lub grupom lokalnym.

Informacje o dodawaniu konta administracyjnego do serwera zarządzania można znaleźć w sekcji "Dodawanie kont administracyjnych" (s. 670).

Role kont administracyjnych

Każde konto administracyjne ma przypisaną rolę ze wstępnie zdefiniowanymi prawami, które są niezbędne do wykonywania określonych zadań. Możliwe są następujące role kont

administracyjnych:

- **Administrator**
  Ta rola zapewnia pełny dostęp administracyjny do organizacji lub jednostki.
- **Tylko do odczytu**
  Ta rola zapewnia dostęp do konsoli internetowej Cyber Protect z uprawnieniem tylko do odczytu. Pozwala ona jedynie na zbieranie danych diagnostycznych, na przykład raportów systemowych. Rola Tylko do odczytu nie pozwala na przeglądanie kopii zapasowych ani zawartości skrzynek pocztowych uwzględnionych w kopii zapasowej.
- **Inspektor**
  Ta rola zapewnia dostęp do karty **Działania** w konsoli internetowej Cyber Protect. Dodatkowe informacje na temat tej karty można znaleźć w sekcji "Karta Działania" (s. 612). Ta rola nie pozwala na zbieranie ani eksportowanie żadnych danych, w tym informacji o systemie serwera zarządzania.

Wszelkie zmiany w ramach ról są wyświetlane na karcie **Działania**.

Dziedziczenie ról

Role z jednostki nadrzędnej są dziedziczone przez jej jednostki podrzędne. Jeśli to samo konto użytkownika ma inne role przypisane w jednostce nadrzędnej, a inne w jednostce podrzędnej, będzie miało obie grupy ról.

Ponadto role mogą być wprost przypisywane do określonego konta użytkownika lub dziedziczone po grupie użytkowników. W ten sposób konto użytkownika może mieć zarówno rolę przypisaną, jak i odziedziczoną.

Jeśli konto użytkownika ma różne role (przypisane i/lub odziedziczone), może uzyskiwać dostęp do obiektów dozwolonych przez którąkolwiek z tych ról i wykonywać na nich działania dozwolone przez którąkolwiek z tych ról. Na przykład konto użytkownika z przypisaną rolą Tylko do odczytu i odziedziczoną rolą Administrator będzie miało prawa administratora.

Ważne
W konsoli internetowej Cyber Protect wyświetlane są tylko role wprost przypisane w ramach bieżącej jednostki. Ewentualne rozbieżności w stosunku do ról odziedziczonych nie są wyświetlane. Zdecydowanie zalecamy przypisywanie ról Administrator, Tylko do odczytu i Inspektor osobnym kontom lub grupom w celu uniknięcia ewentualnych problemów z rolami odziedziczonymi.

Administratorzy domyślni

W systemie Windows

Gdy serwer zarządzania jest instalowany na komputerze, zachodzą następujące zdarzenia:

- Grupa użytkowników **Acronis Centralized Admins** jest tworzona na komputerze.
  Na kontrolerze domeny grupa ta ma nazwę *DCNAME* **$ Acronis Centralized Admins**. *DCNAME* oznacza tu nazwę NetBIOS kontrolera domeny.
- Wszyscy członkowie grupy **Administratorzy** zostaną dodani do grupy **Acronis Centralized Admins**. Jeśli komputer znajduje się w domenie, ale nie jest jej kontrolerem, lokalni (niedomenowi) użytkownicy zostaną wykluczeni. Na kontrolerze domeny nie ma żadnych niedomenowych użytkowników.
- Grupy **Acronis Centralized Admins** i **Administratorzy** zostaną dodane do serwera zarządzania jako **administratorzy organizacji**. Jeśli komputer znajduje się w domenie, ale nie jest jej kontrolerem, grupa **Administratorzy** nie zostanie dodana, w związku z czym lokalni (niedomenowi) użytkownicy nie zostaną administratorami organizacji.

Możesz usunąć grupę **Administratorzy** z listy administratorów organizacji. Nie można jednak usunąć grupy **Acronis Centralized Admins**. W mało prawdopodobnym przypadku usunięcia wszystkich administratorów organizacji możesz dodać konto do grupy **Acronis Centralized Admins** w systemie Windows, a następnie zalogować się do konsoli internetowej Cyber Protect przy użyciu tego konta.

W systemie Linux

Podczas instalacji serwera zarządzania na komputerze dodawany jest do niego użytkownik **root** jako **administrator organizacji**.

Do listy administratorów serwera zarządzania można też dodać innych użytkowników systemu Linux, zgodnie z opisem zamieszczonym w dalszej części tego dokumentu, a następnie usunąć użytkownika **root** z tej listy. W mało prawdopodobnym przypadku usunięcia wszystkich administratorów organizacji można uruchomić ponownie usługę `acronis_asm`. W wyniku tej operacji użytkownik **root** zostanie automatycznie ponownie dodany jako administrator organizacji.

Konto administracyjne w wielu jednostkach

Kontu można przyznać prawa administracyjne w dowolnej liczbie jednostek. W przypadku takiego konta, a także kont administracyjnych na poziomie organizacji, w konsoli internetowej Cyber Protect jest wyświetlany selektor jednostek. Przy użyciu tego selektora na koncie można wyświetlać każdą jednostkę z osobna i nią zarządzać.

Konto mające uprawnienia w przypadku wszystkich jednostek w organizacji nie ma uprawnień dotyczących organizacji. Konta administracyjne na poziomie organizacji muszą zostać jawnie dodane do grupy **Organizacja**.

Jak zapełnić jednostki komputerami

Gdy administrator doda komputer za pośrednictwem interfejsu internetowego, komputer zostanie dodany do jednostki zarządzanej przez administratora. Jeśli administrator zarządza wieloma jednostkami, komputer jest dodawany do jednostki wybranej w selektorze jednostek. W związku z tym administrator musi wybrać jednostkę zanim kliknie **Dodaj**.

Podczas lokalnego instalowania agentów administrator podaje ich poświadczenia. Komputer zostanie dodany do jednostki zarządzanej przez administratora. Jeśli administrator zarządza wieloma jednostkami, instalator wyświetli monit o wybranie jednostki, do której komputer zostanie dodany.

Dodawanie kont administracyjnych

Uwaga
Ta funkcja jest niedostępna w wersji Standard i Essentials.

Aby dodać konta

1. Kliknij **Ustawienia** > **Konta**.
   W oprogramowaniu zostanie wyświetlona lista administratorów serwera zarządzania i drzewo jednostek (o ile istnieje).
2. Wybierz **Organizację** lub wybierz jednostkę, do której chcesz dodać administratora.
3. Kliknij **Dodaj konto**.
4. W obszarze **Domena** wybierz domenę zawierającą konta użytkowników, które chcesz dodać. Jeśli serwer zarządzania nie znajduje się w domenie Active Directory lub jest zainstalowany w systemie Linux, można dodać tylko użytkowników lokalnych.
5. Wyszukaj nazwę użytkownika lub grupy użytkowników.
6. Kliknij znak „+” obok nazwy użytkownika lub grupy.
7. Wybierz rolę konta.
8. Powtórz kroki 4–6 dla wszystkich użytkowników lub grup, które chcesz dodać.
9. Po zakończeniu kliknij **Gotowe**.
10. [Tylko w systemie Linux] Dodaj nazwy użytkowników do konfiguracji modułu Linux Pluggable Authentication Module (PAM) dotyczącej modułów rozwiązania firmy Acronis zgodnie z poniższym opisem.

Aby dodać nazwy użytkowników do konfiguracji modułu PAM dotyczącej rozwiązania firmy Acronis

Ta procedura dotyczy serwerów zarządzania działających na komputerach z systemem Linux oraz na maszynach wirtualnych Acronis Cyber Protect All-in-One Appliance.

1. Na komputerze z serwerem zarządzania jako użytkownik root otwórz plik **/etc/security/acronisagent.conf** w edytorze tekstowym.
2. W pliku tym wpisz nazwy użytkowników dodanych jako administratorzy serwera zarządzania — każdą w osobnym wierszu.
3. Zapisz i zamknij plik.

Tworzenie jednostek

1. Kliknij **Ustawienia** > **Konta**.
2. W oprogramowaniu zostanie wyświetlona lista administratorów serwera zarządzania i drzewo jednostek (o ile istnieje).
3. Wybierz **Organizacja** lub wybierz jednostkę nadrzędną nowej jednostki.
4. Kliknij **Utwórz jednostkę**.
5. Określ nazwę nowej jednostki, a następnie kliknij **Utwórz**.

Wdrożenie chmurowe

Funkcje administrowania kontami użytkowników i jednostkami organizacyjnymi są dostępne w portalu zarządzania. Aby uzyskać dostęp do portalu zarządzania, kliknij **Portal zarządzania** podczas logowania się do usługi Cyber Protection lub ikonę  w prawym górnym rogu, a następnie kliknij **Portal zarządzania**. Dostęp do portalu mają tylko użytkownicy z uprawnieniami administracyjnymi.

Aby uzyskać informacje na temat administrowania kontami użytkowników i jednostkami organizacyjnymi, zobacz Podręcznik administratora portalu zarządzania. W celu uzyskania dostępu do tego dokumentu kliknij ikonę ze znakiem zapytania w portalu zarządzania.

W tej sekcji zamieszczono dodatkowe informacje dotyczące zarządzania usługą Cyber Protection.

Limity

Limity pozwalają ograniczać możliwość użytkowników do korzystania z usługi. Aby ustawić te limity, wybierz użytkownika na karcie **Użytkownicy**, a następnie kliknij ikonę ołówka w sekcji **Limity**.

W przypadku przekroczenia limitu na adres e-mail użytkownika jest wysyłane stosowne powiadomienie. Jeśli nie ustawisz nadwyżki limitu, limit jest uznawany za „elastyczny”. Oznacza to, że ograniczenia dotyczące korzystania z usługi Cyber Protection nie są stosowane.

Możesz też określić nadwyżki limitów. Nadwyżka umożliwia użytkownikowi przekroczenie limitu o określoną wartość. W przypadku przekroczenia nadwyżki zostaną zastosowane ograniczenia dotyczące korzystania z usługi Cyber Protection.

Kopia zapasowa

Możesz określić limit miejsca w chmurze, limit lokalnych kopii zapasowych oraz maksymalną liczbę komputerów, urządzeń lub skrzynek pocztowych, które może chronić użytkownik. Dostępne są następujące limity:

- **Chmura**
- **Stacje robocze**
- **Serwery**

- **Windows Server Essentials**
- **Hosty wirtualne**
- **Uniwersalny**
  Tego limitu można używać zamiast któregokolwiek z czterech limitów wymienionych powyżej: Stacje robocze, Serwery, Windows Server Essentials, Hosty wirtualne.
- **Urządzenia mobilne**
- **Skrzynki pocztowe Microsoft 365**
- **Lokalne kopie zapasowe**

Komputer, urządzenie lub skrzynka pocztowa są uznawane za chronione, gdy jest do nich stosowany co najmniej jeden plan ochrony. Urządzenie mobilne staje się chronione po utworzeniu pierwszej kopii zapasowej.

W przypadku przekroczenia nadwyżki limitu miejsca w chmurze tworzenie kopii zapasowej zakończy się niepowodzeniem. W przypadku przekroczenia nadwyżki liczby urządzeń użytkownik nie może zastosować planu ochrony do kolejnych urządzeń.

Limit **Lokalnych kopii zapasowych** ogranicza łączny rozmiar lokalnych kopii zapasowych tworzonych za pomocą infrastruktury chmury. Dla tego limitu nie można ustawić nadwyżki.

Odzyskiwanie po awarii

Dostawca usługi stosuje te limity dla całej firmy. Administratorzy firmy mogą przeglądać limity oraz monitorować wykorzystanie w portalu zarządzania, ale nie mogą ustawiać limitów użytkowników.

- **Magazyn odzyskiwania po awarii**
  Ten magazyn jest używany przez serwery podstawowe i serwery odzyskiwania. W przypadku osiągnięcia nadwyżki tego limitu nie można tworzyć serwerów podstawowych i serwerów odzyskiwania ani dodawać/rozszerzać dysków istniejących serwerów podstawowych. W przypadku przekroczenia nadwyżki tego limitu nie można inicjować przełączenia awaryjnego ani uruchamiać zatrzymanego serwera. Działające serwery kontynuują pracę.
  W przypadku wyłączenia limitu wszystkie serwery są usuwane. Karta **Lokalizacja odzyskiwania w chmurze** zniknie z konsoli internetowej Cyber Protect.
- **Punkty obliczeniowe**
  Limit ogranicza zasoby procesora i pamięci RAM wykorzystywane przez serwery podstawowe oraz serwery odzyskiwania podczas okresu rozliczeniowego. W przypadku osiągnięcia nadwyżki tego limitu wszystkie serwery podstawowe i serwery odzyskiwania są wyłączane. Nie można użyć tych serwerów aż do rozpoczęcia następnego okresu rozliczeniowego. Domyślny okres rozliczeniowy to pełny miesiąc kalendarzowy.
  W przypadku wyłączenia tego limitu nie można korzystać z serwerów — niezależnie od okresu rozliczeniowego.
- **Publiczne adresy IP**

Limit ogranicza liczbę publicznych adresów IP, które można przypisać do serwerów głównych i serwerów odzyskiwania. W przypadku osiągnięcia nadwyżki tego limitu nie można włączać publicznych adresów IP dla kolejnych serwerów. Możesz zablokować możliwość używania publicznego adresu IP na danym serwerze, odznaczając pole wyboru **Publiczny adres IP** w ustawieniach serwera. Następnie możesz pozwolić innemu serwerowi używać publicznego adresu IP, który najczęściej będzie inny.

W przypadku wyłączenia tego limitu wszystkie serwery przestają używać publicznych adresów IP, przez co stają się niedostępne z Internetu.

- **Serwery chmurowe**

  Ten limit ogranicza łączną liczbę serwerów podstawowych i serwerów odzyskiwania. W przypadku osiągnięcia nadwyżki tego limitu nie można tworzyć serwerów głównych ani serwerów odzyskiwania.

  W razie wyłączenia limitu serwery są widoczne w konsoli internetowej Cyber Protect, ale dostępna jest jedynie operacja **Usuń**.
- **Dostęp do Internetu**

  Ten limit powoduje włączenie lub wyłączenie dostępu do Internetu z serwerów głównych i serwerów odzyskiwania.

  W razie wyłączenia limitu serwery główne i serwery odzyskiwania są natychmiast odłączane od internetu. Przełącznik **Dostęp do Internetu** w oknie właściwości serwerów staje się nieaktywny.

Powiadomienia

Aby zmienić ustawienia powiadomień dla użytkownika, wybierz go na karcie **Użytkownicy**, a następnie kliknij ikonę ołówka w sekcji **Ustawienia**. Dostępne są następujące ustawienia powiadomień:

- **Powiadomienia o nadużyciu limitów** (domyślnie włączone)

  Powiadomienia o przekroczeniu limitów.
- **Zaplanowane raporty z wykorzystania**

  Opisane poniżej raporty z wykorzystania, które są wysyłane pierwszego dnia każdego miesiąca.
- **Powiadomienia o błędach**, **Powiadomienia o ostrzeżeniach** oraz **Powiadomienia o udanych operacjach** (domyślnie wyłączone)

  Powiadomienia o wynikach wykonywania planów ochrony oraz operacji odzyskiwania po awarii dla każdego urządzenia.
- **Codziennie zestawienie aktywnych alertów** (domyślnie włączone)

  Jest to zestawienie z informacjami nie tylko o niepowodzeniu tworzenia kopii zapasowych, ale również o brakujących kopiach zapasowych i innych problemach. Zestawienie jest wysyłane o 10:00 (czas centrum danych). Jeśli nie wystąpiły żadne problemy, zestawienie nie jest wysyłane.

Wszystkie powiadomienia są wysyłane na adres e-mail użytkownika.

Raporty

Raport dotyczący korzystania z usługi Cyber Protection obejmuje następujące dane o organizacji lub jednostce:

- Rozmiar kopii zapasowych według jednostki, użytkownika i typu urządzenia.
- Liczba chronionych urządzeń według jednostki, użytkownika i typu urządzenia.
- Cena według jednostki, użytkownika i typu urządzenia.
- Łączny rozmiar kopii zapasowych.
- Łączna liczba chronionych urządzeń.
- Łączna wartość cenowa.

Opis wiersza poleceń

Wykaz poleceń wiersza polecenia to osobny dokument dostępny pod adresem https://www.acronis.com/en-us/support/documentation/AcronisCyberProtect_15_Command_Line_Reference/index.html.

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. Wykonaj jedną z następujących czynności:
   - W obszarze **Urządzenia** wybierz komputer, z którego chcesz zebrać dzienniki, a następnie kliknij **Działania**.
   - W obszarze **Ustawienia** > **Agenci** wybierz komputer, z którego chcesz zebrać dzienniki, a następnie kliknij **Szczegóły**.
2. Kliknij **Zbierz informacje o systemie**.
3. Jeśli przeglądarka wyświetli monit, określ, gdzie ma zostać zapisany plik.

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. Ten format jednoplikowej kopii zapasowej nie jest dostępny w przypadku wykonywania kopii zapasowej do lokalizacji nieobsługujących odczytu i zapisu z dostępem losowym, takich jak serwery SFTP.

L

Lokalizacja zarządzana

Lokalizacja kopii zapasowej zarządzana przez węzeł magazynowania. Lokalizacje zarządzane mogą się fizycznie znajdować w udziale sieciowym, systemie SAN, udziale NAS, na lokalnym dysku twardym węzła magazynowania lub w bibliotece taśm podłączonej lokalnie do węzła magazynowania. Węzeł magazynowania wykonuje zadania czyszczenia oraz sprawdzania poprawności (jeśli są uwzględnione w planie ochrony) w odniesieniu do każdej kopii zapasowej przechowywanej w lokalizacji zarządzanej. Możesz określać dodatkowe operacje, które ma wykonywać węzeł magazynowania (takie jak deduplikacja czy szyfrowanie).

P

Pełna kopia zapasowa

Samowystarczalna kopia zapasowa zawierająca wszystkie dane wybrane do uwzględnienia w niej. 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

W różnicowej kopii zapasowej są przechowywane tylko dane zmienione względem ostatniej pełnej kopii zapasowej. Aby odzyskać dane z różnicowej kopii zapasowej, należy uzyskać dostęp do odpowiedniej pełnej kopii zapasowej.

S

Startup Recovery Manager

Zmodyfikowana wersja agenta startowego znajdująca się na dysku systemowym, uruchamiana po naciśnięciu klawisza F11 podczas uruchamiania komputera. Program Startup Recovery Manager eliminuje potrzebę użycia nośnika ratunkowego lub połączenia sieciowego w celu uruchomienia ratunkowego

narzędzia startowego. Program Startup Recovery Manager przydaje się szczególnie użytkownikom mobilnym. W razie awarii należy ponownie uruchomić komputer, nacisnąć klawisz F11 po wyświetleniu monitu „Naciśnij klawisz F11, aby uruchomić program Startup Recovery Manager" i odzyskać dane tak samo jak ze zwykłego nośnika startowego. Ograniczenie: wymaga ponownej aktywacji programów ładujących (nie dotyczy programu ładującego systemu Windows i GRUB).

Z

Zestaw kopii zapasowych

Grupa kopii zapasowych, do których można zastosować odrębną regułę przechowywania. W przypadku niestandardowego schematu tworzenia kopii zapasowych 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. 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 zapasowa. Jeśli tygodniowa kopia zapasowa jest pierwszą kopią zapasową utworzoną po rozpoczęciu miesiąca, jest ona uznawana za miesięczną kopię zapasową. W takiej sytuacji tygodniowa kopia zapasowa zostanie utworzona w wybrany dzień następnego tygodnia. Dzienną kopią zapasową jest pierwsza kopia zapasowa utworzona po rozpoczęciu dnia, chyba że spełnia warunki definicji miesięcznej lub tygodniowej kopii zapasowej. Godzinną kopią zapasową jest pierwsza kopia zapasowa utworzona po rozpoczęciu godziny, chyba że spełnia warunki definicji miesięcznej, tygodniowej lub dziennej kopii zapasowej.

Indeks

J

K

R

S

T

U

W

Z

Ź