

Contents

Omówienie

Data Protection Manager

Jak działa program DPM?

Co program DPM może umieścić w kopii zapasowej?

Biblioteki taśm zgodne z programem DPM

Wprowadzenie

Wersje kompilacji programu DPM

Informacje o wersji programu DPM

Co nowego w programie DPM

Co obsługuje program DPM

Procedura

Planowanie środowiska programu DPM

Przygotowanie do wdrożenia serwerów programu DPM

Przygotowywanie środowiska dla programu DPM

Przygotowanie magazynu danych

Określanie zgodnych bibliotek taśm

Określanie źródeł danych, które mają być chronione

Instalowanie lub uaktualnianie programu DPM

Instalowanie programu DPM

Uaktualnianie instalacji programu DPM

Dodawanie magazynu za pomocą funkcji Modern Backup Storage

Deduplikacja magazynu programu DPM

Wdrażanie programu DPM

Wdrażanie agenta ochrony programu DPM

Wdrażanie grup ochrony

Konfigurowanie ustawień zapory

Kopia zapasowa offline

Korzystanie z własnego dysku

Ochrona obciążeń

Tworzenie kopii zapasowych maszyn wirtualnych funkcji Hyper-V

Tworzenie kopii zapasowej programu Exchange przy użyciu programu DPM

Tworzenie kopii zapasowej programu SharePoint przy użyciu programu DPM

Tworzenie kopii zapasowej programu SQL Server za pomocą programu DPM

Tworzenie kopii zapasowej komputerów klienckich przy użyciu programu DPM

Tworzenie kopii zapasowej danych plików przy użyciu programu DPM

Tworzenie kopii zapasowej stanu systemu i kompletnego stanu systemu

Tworzenie i przywracanie kopii zapasowej serwerów VMware

Tworzenie i przywracanie kopii zapasowej serwerów VMM

Przygotowanie do tworzenia kopii zapasowej ogólnego źródła danych

Przygotowywanie komputerów w grupach roboczych i domenach niezaufanych na potrzeby tworzenia kopii zapasowych

Tworzenie kopii zapasowej serwera DPM

Monitorowanie i zarządzanie

Monitorowanie programu DPM

Konfigurowanie rejestrowania w programie DPM

Generowanie raportów programu DPM

Zarządzanie serwerami programu DPM i monitorowanie ich za pomocą programu SCOM

Poprawianie wydajności replikacji

Zarządzanie serwerami DPM za pomocą konsoli centralnej

Data Protection Manager

11.12.2019 • 3 minutes to read

Każda organizacja potrzebuje strategii dotyczącej ciągłości działania i odzyskiwania danych po awarii (BCDR, business continuity and disaster recovery), aby zapewnić dostępność zasobów w trakcie planowanych i nieplanowanych przestojów oraz aby upewnić się, że po awarii możliwe będzie ponowne rozpoczęcie działania w normalnych warunkach. Strategia BCDR wymaga zapewnienia bezpieczeństwa danych i możliwości ich odzyskiwania oraz utrzymywania stałej dostępności usług, aplikacji i obciążeń biznesowych. Program System Center Data Protection Manager (DPM) to niezawodny system klasy korporacyjnej umożliwiający tworzenie kopii zapasowych i odzyskiwanie danych. Jest on elementem strategii BCDR, ponieważ obsługuje tworzenie kopii zapasowych i odzyskiwanie danych przedsiębiorstwa.

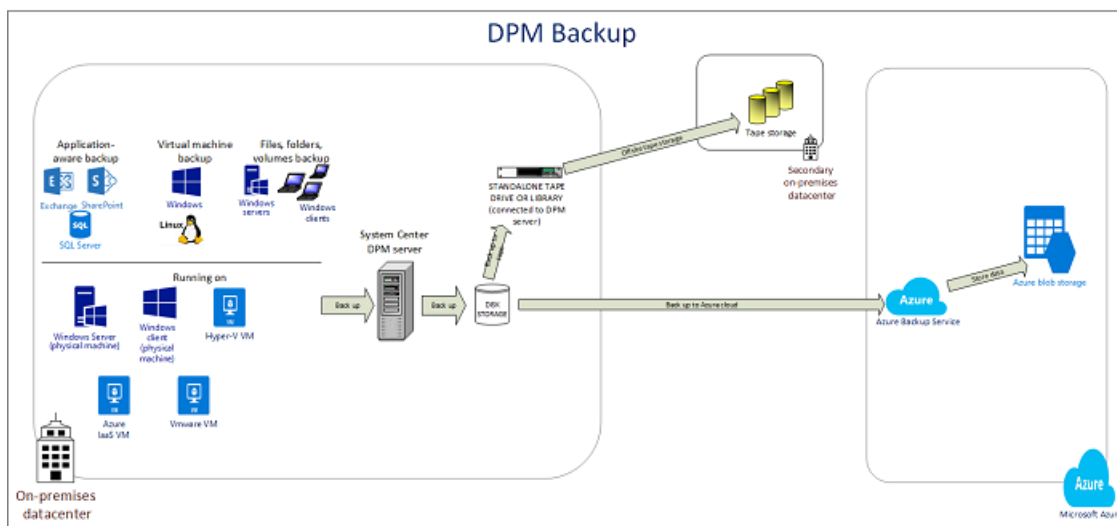
Program System Center Data Protection Manager (DPM) można wdrożyć dla:

- **Kopia zapasowa obsługująca aplikacje:** tworzenie obsługujących aplikacje kopii zapasowych obciążeń firmy Microsoft, w tym programów SQL Server, Exchange oraz SharePoint.
- **Kopia zapasowa plików:** tworzenie kopii zapasowych plików, folderów i woluminów komputerów z serwerowymi i klienckimi systemami operacyjnymi Windows.
- **Kopia zapasowa systemu:** tworzenie kopii zapasowych stanu systemu lub kopii zapasowej z możliwością odzyskiwania systemu od zera dla komputerów fizycznych z serwerowymi lub klienckimi systemami operacyjnymi Windows.
- **Kopia zapasowa funkcji Hyper-V:** tworzenie kopii zapasowych maszyn wirtualnych funkcji Hyper-V z systemem Windows lub Linux. Można utworzyć kopię zapasową całej maszyny wirtualnej lub uruchamiać tworzenie obsługujących aplikacje kopii zapasowych obciążeń firmy Microsoft na maszynach wirtualnych funkcji Hyper-V z systemem Windows.
- Pełną listę można znaleźć w temacie [Co program DPM może umieścić w kopii zapasowej?](#)

Miejsca, w których program DPM może przechowywać dane kopii zapasowej, to:

- **Dysk:** w celu przechowywania krótkoterminowego program DPM tworzy kopie zapasowe danych w pulach dysków.
- **Platforma Azure:** w celu krótko- i długoterminowego przechowywania poza siedzibą firmy można utworzyć kopię zapasową zapisanych w pulach dysków danych programu DPM w chmurze platformy Microsoft Azure za pomocą usługi Azure Backup.
- **Taśma:** w celu przechowywania długoterminowego można utworzyć kopię zapasową danych na taśmie, którą następnie można umieścić poza siedzibą firmy.

Jeśli wystąpiły awarie i źródło danych jest niedostępne, za pomocą programu DPM można łatwo przywrócić dane do oryginalnego źródła lub lokalizacji alternatywnej. W ten sposób, jeśli oryginalne dane są niedostępne z powodu planowanych lub nieoczekiwanych sytuacji, można je łatwo przywrócić z lokalizacji alternatywnej. Program DPM używa programu SQL Server jako bazy danych, a użytkownik może chronić serwer programu DPM na potrzeby odzyskiwania sprawności po awarii. Poniższy diagram zawiera omówienie funkcji tworzenia kopii zapasowych w programie DPM.



Następne kroki

Dowiedz się więcej w temacie [How DPM works?](#) (Jak działa program DPM?)

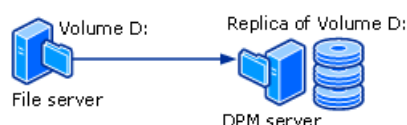
Jak działa program DPM?

11.12.2019 • 23 minutes to read

Metoda System Center Data Protection Manager (DPM) używa do ochrony danych w zależności od typu chronionych danych i wybranej metody ochrony. W tym artykule znajdują się podstawowe informacje dotyczące działania programu DPM. Przeznaczony jest on dla nowych użytkowników programu DPM oraz dla tych, którzy chcieliby uzyskać odpowiedzi na podstawowe pytania dotyczące tego, *jak* działa program DPM. W tym artykule omówiono procesy ochrony opartej na dyskach, procesy ochrony opartej na taśmach, proces odzyskiwania, a także zasady ochrony.

Proces ochrony opartej na dyskach

Aby zapewnić ochronę danych na dysku, serwer programu DPM tworzy i przechowuje replikę lub kopię danych znajdujących się na serwerach chronionych. Repliki są przechowywane w puli magazynów, która składa się z zestawu dysków znajdujących się na serwerze programu DPM lub na woluminie niestandardowym. Na poniższej ilustracji przedstawiono podstawowe relacje między woluminem chronionym i jego repliką.



Niezależnie od tego, czy chronione są dane pliku, czy dane aplikacji, ochrona zaczyna się od utworzenia repliki źródła danych.

Replika jest synchronizowana lub aktualizowana w regularnych odstępach czasu zgodnie ze skonfigurowanymi ustawieniami. Metoda, jaką posługuje się program DPM w celu synchronizacji repliki zależy od typu chronionych danych. Aby uzyskać więcej informacji, zobacz Proces synchronizowania danych pliku oraz Proces synchronizowania danych aplikacji. Jeśli replika jest zidentyfikowana jako niespójna, program DPM przeprowadza sprawdzanie spójności, czyli weryfikację repliki blok po bloku w odniesieniu do źródła danych.

Prosty przykład konfiguracji ochrony składa się z serwera programu DPM i komputera chronionego. Komputer jest chroniony po zainstalowaniu agenta ochrony programu DPM na komputerze i dodaniu jego danych do grupy ochrony.

Agenci ochrony śledzą zmiany w chronionych danych i przesyłają je do serwera programu DPM. Agent ochrony identyfikuje również dane na komputerze, które mogą być chronione i są zaangażowane w proces odzyskiwania. Agentów ochrony należy zainstalować na wszystkich komputerach, które mają być chronione przy użyciu programu DPM. Agentów ochrony można zainstalować za pomocą programu DPM lub ręcznie przy użyciu aplikacji, takich jak Systems Management Server (SMS).

Grupy ochrony są używane do zarządzania ochroną źródeł danych na komputerach. Grupa ochrony to kolekcja źródeł danych, które mają taką samą konfigurację ochrony. Konfiguracja ochrony jest kolekcją ustawień, które są wspólne dla grupy ochrony, a wśród nich można wymienić: nazwę grupy ochrony, zasady ochrony, przydziały dysków i metodę tworzenia repliki.

Program DPM przechowuje oddzielną replikę dla każdego członka grupy ochrony w puli magazynu. Członkiem grupy ochrony może być dowolne z następujących źródeł danych:

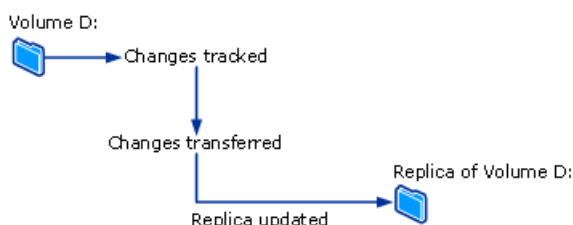
- Wolumin, udział lub folder na komputerze stacjonarnym, serwerze plików lub w klastrze serwerów.
- Grupa magazynów na serwerze programu Exchange lub w klastrze serwerów
- Baza danych wystąpienia serwera programu SQL Server lub klastra serwerów

NOTE

Program DPM nie chroni danych przechowywanych na dyskach USB.

Proces synchronizacji danych plików

W przypadku woluminu lub udziału plików na serwerze agent ochrony programu DPM używa filtra woluminu i dziennika zmian w celu stwierdzenia, które pliki uległy zmianie, a następnie oblicza sumę kontrolną tych plików, aby zsynchronizować tylko zmodyfikowane bloki. W trakcie synchronizacji zmiany są przesyłane na serwer programu DPM, a następnie stosowane do repliki w celu jej zsynchronizowania ze źródłem danych. Na poniższym rysunku przedstawiono proces synchronizowania plików.



Jeśli replika stanie się niespójna ze źródłem danych, program DPM wygeneruje alert określający, którego komputera i których źródeł danych dotyczy problem. Aby go rozwiązać, administrator naprawia replikę, inicjując synchronizację repliki z kontrolą spójności. W ramach kontroli spójności program DPM przeprowadza weryfikację blok po bloku i naprawia replikę tak, aby była spójna ze źródłami danych.

Można zaplanować codzienną kontrolę spójności grup ochrony lub inicjować ją ręcznie.

Program DPM tworzy punkt odzyskiwania członka grupy ochrony w konfigurowalnych, regularnych odstępach czasu. Punkt odzyskiwania jest wersją danych, przy użyciu którego można odzyskać dane.

Proces synchronizacji danych aplikacji

W przypadku danych aplikacji po utworzeniu repliki przez program DPM zmiany bloków woluminu należących do plików aplikacji są śledzone przez filtr woluminu.

Sposób przekazywania zmian do serwera programu DPM zależy od aplikacji i typu synchronizacji. Operacja oznakowana jako synchronizacja w konsoli administratora programu DPM jest porównywalna do przyrostowej kopii zapasowej i w połączeniu z repliką dokładnie odzwierciedla dane aplikacji.

W trakcie przeprowadzania synchronizacji oznaczonej jako ekspresowa pełna kopia zapasowa w konsoli administratora programu DPM jest tworzona pełna migawka usługi kopiowania woluminów w tle (VSS), ale do serwera programu DPM są wysyłane tylko zmodyfikowane bloki.

Każda ekspresowa pełna kopia zapasowa tworzy punkt odzyskiwania danych aplikacji. Jeśli aplikacja obsługuje tworzenie przyrostowych kopii zapasowych, punkt odzyskiwania jest również tworzony przy każdej synchronizacji. Typ synchronizacji obsługiwany przez każdy z typów danych aplikacji można podsumować w następujący sposób:

- W przypadku chronionych danych programu Exchange funkcja synchronizacji transferuje przyrostową migawkę usługi VSS przy użyciu składnika zapisywania usługi VSS programu Exchange. Punkty odzyskiwania są tworzone dla wszystkich synchronizacji i ekspresowych pełnych kopii zapasowych.
- Bazy danych serwera SQL wysłane z dziennikiem, w trybie tylko do odczytu lub korzystające z modelu odzyskiwania prostego nie obsługują tworzenia przyrostowej kopii zapasowej. Punkty odzyskiwania są tworzone tylko dla wszystkich ekspresowych pełnych kopii zapasowych. W przypadku wszystkich innych baz danych serwera SQL funkcja synchronizacji transferuje kopię zapasową dziennika transakcji, a następnie są tworzone punkty odzyskiwania dla wszystkich synchronizacji przyrostowych i ekspresowych pełnych kopii zapasowych. Dziennik transakcji jest rekordem sekwencyjnym wszystkich transakcji przeprowadzonych wobec bazy danych od czasu utworzenia ostatniej kopii zapasowej dziennika transakcji.

- Programy Windows SharePoint Services i Microsoft Virtual Server nie obsługują tworzenia przyrostowych kopii zapasowych. Punkty odzyskiwania są tworzone tylko dla wszystkich ekspresowych pełnych kopii zapasowych.

Synchronizacje przyrostowe wymagają mniej czasu od wykonania ekspresowej pełnej kopii zapasowej. Czas wymagany do odzyskania danych zwiększa się jednak wraz z liczbą synchronizacji. Dzieje się tak, ponieważ program DPM musi przywrócić ostatnią pełną kopię zapasową, a następnie przywrócić i zastosować wszystkie synchronizacje przyrostowe do momentu określonego do odzyskania.

Aby skrócić czas odzyskiwania, program DPM tworzy regularnie ekspresową pełną kopię zapasową, która jest typem synchronizacji aktualizującym replikę tak, aby zawierała zmodyfikowane bloki.

Podczas tworzenia ekspresowej pełnej kopii zapasowej program DPM tworzy migawkę repliki przed jej zaktualizowaniem zmodyfikowanymi blokami. Aby umożliwić częstsze osiąganie celów punktów odzyskiwania i zmniejszyć okno utraty danych, program DPM wykonuje również synchronizacje przyrostowe w okresie między dwiema ekspresowymi pełnymi kopiami zapasowymi.

Tak jak w przypadku ochrony danych plików, jeśli replika stanie się niespójna ze źródłem danych, program DPM wygeneruje alert określający, którego serwera i źródła danych dotyczy problem. Aby go rozwiązać, administrator naprawia replikę, inicjując synchronizację repliki z kontrolą spójności. W ramach kontroli spójności program DPM przeprowadza weryfikację blok po bloku i naprawia replikę tak, aby była spójna ze źródłami danych.

Można zaplanować codzienną kontrolę spójności grup ochrony lub inicjować ją ręcznie.

Różnica między danymi plików i danymi aplikacji

Dane znajdujące się na serwerze plików, które trzeba chronić jako plik prosty, zaliczamy do danych pliku, np. pliki pakietu Microsoft Office, pliki tekstowe, pliki wsadowe, itp.

Dane znajdujące się na serwerze aplikacji, które wymagają przesłania informacji o aplikacji do programu DPM, zaliczamy do danych aplikacji, np. grupy magazynu programu Exchange, bazy danych programu SQL Server, farmy programu Windows SharePoint Services i programu Virtual Server.

Każde źródło danych jest prezentowane w konsoli administratora programu DPM zgodnie z typem ochrony, który można wybrać dla tego źródła danych. Na przykład w Kreatorze tworzenia nowej grupy ochrony, rozszerzając serwer, który zawiera pliki, a także dział z programem Virtual Server i wystąpieniem programu SQL Server, źródła danych są traktowane w następujący sposób:

- Po rozwinięciu pola Wszystkie udziały lub Wszystkie woluminy program DPM wyświetla udziały i woluminy na tym serwerze i będzie chronić dowolne źródło danych wybrane w jednym z tych węzłów jako dane pliku.
- Po rozwinięciu pola Wszystkie serwery SQL program DPM wyświetla wystąpienia programu SQL Server na tym serwerze i będzie chronić dowolne źródło danych wybrane w tym węźle jako dane aplikacji.
- Po rozwinięciu pola Microsoft Virtual Server program DPM wyświetla wystąpienia programu SQL Server na tym serwerze i będzie chronić dowolne źródło danych wybrane w tym węźle jako dane aplikacji.

Proces ochrony opartej na taśmach

Jeśli używasz krótkoterminowej ochrony opartej na dyskach i długoterminowej ochrony opartej na taśmach, program DPM może wykonać kopię zapasową danych z woluminu repliki na taśmę, bez wywierania wpływu na komputer chroniony. Jeśli korzystasz tylko z ochrony opartej na taśmie, program DPM tworzy kopie zapasowe danych bezpośrednio z komputera chronionego na taśmę.

Program DPM chroni dane na taśmach przy użyciu kombinacji pełnych i przyrostowych kopii zapasowych tworzonych z chronionego źródła danych (ochrona krótkoterminowa na taśmach lub ochrona długoterminowa na taśmach, jeśli program DPM nie chroni danych na dysku) lub z repliki programu DPM (ochrona krótkoterminowa

na taśmie, natomiast ochronę długoterminową zapewnia dysk).

NOTE

Jeśli plik był otwarty podczas ostatniej synchronizacji repliki, kopia zapasowa tego pliku z repliki będzie w stanie spójnym awarii. Stan spójny awarii pliku będzie zawierał wszystkie dane z pliku, który został zachowany na dysku w czasie ostatniej synchronizacji. Dotyczy to tylko kopii zapasowych systemu plików. Kopie zapasowe aplikacji zawsze będą zgodne ze stanem aplikacji.

Więcej na temat poszczególnych typów kopii zapasowej i harmonogramów znajduje się w temacie Planowanie grup ochrony

Proces odzyskiwania

Metoda ochrony danych na dysku lub na taśmie nie ma wpływu na zadania odzyskiwania. Wybierz punkt odzyskiwania danych, które chcesz odzyskać, a program DPM przywróci dane na komputerze chronionym.

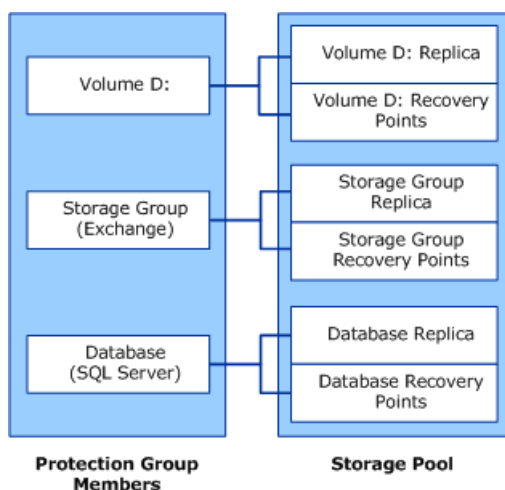
Program DPM może przechowywać maksymalnie 64 punktów odzyskiwania dla każdego członka pliku należącego do grupy ochrony. W przypadku źródeł danych aplikacji program DPM może przechowywać maksymalnie 448 ekspresowych pełnych kopii zapasowych oraz maksymalnie 96 przyrostowych kopii zapasowych dla każdej ekspresowej pełnej kopii zapasowej. Jeśli limity obszaru magazynowania zostały osiągnięte, a zakres przechowywania dla istniejących punktów odzyskiwania nie jest jeszcze spełniony, zadania ochrony zakończą się niepowodzeniem.

NOTE

W celu obsługi odzyskiwania przez użytkownika końcowego punkty odzyskiwania dla plików są ograniczone do 64 przez usługę kopiowania woluminów w tle (VSS).

Jak wyjaśniono w artykułach Proces synchronizowania danych pliku i Proces synchronizowania danych aplikacji, proces tworzenia punktów odzyskiwania jest inny w przypadku danych pliku i danych aplikacji. Program DPM tworzy punkty odzyskiwania danych pliku, pobierając kopię w tle z repliki zgodnie ze skonfigurowanym harmonogramem. W przypadku danych aplikacji każda operacja synchronizacji i każde zadanie tworzenia ekspresowej pełnej kopii zapasowej powoduje utworzenie punktu odzyskiwania.

Na poniższej ilustracji przedstawiono, jak każdy członek grupy ochrony jest skojarzony ze swoim woluminem repliki i woluminem punktu odzyskiwania.



Administratorzy odzyskują dane z dostępnych punktów odzyskiwania przy użyciu Kreatora odzyskiwania w konsoli administratora programu DPM. Po wybraniu źródła danych i stałego punktu odniesienia dla zadania odzyskiwania program DPM powiadamia użytkownika, czy dane są na taśmie, czy taśma jest w trybie online czy offline oraz

które taśmy są potrzebne do ukończenia odzyskiwania.

Administratorzy programu DPM mogą zezwolić użytkownikom końcowym na wykonywanie własnych zadań odzyskiwania przy użyciu funkcji starszych wersji w systemie Windows. Jeśli nie chcesz, aby użytkownicy końcowi mieli taką możliwość, odzyskiwanie danych na komputerach stacjonarnych odbywać się będzie za pomocą Kreatora odzyskiwania.

Zasady ochrony

Na podstawie celów odzyskiwania określonych dla grupy ochrony program DPM konfiguruje zasady ochrony lub harmonogram zadań dla tej grupy ochrony. Poniżej podano przykłady celów odzyskiwania:

- "Utrata nie więcej niż 1 godzinę danych produkcyjnych"
- „Zapewnij zakres przechowywania równy 30 dni”
- „Przechowuj dane dostępne do odzyskania przez 7 lat”

Cele odzyskiwania określają ilościowo wymagania dotyczące ochrony danych organizacji. Cele odzyskiwania w programie DPM definiuje się na podstawie zakresu przechowywania, tolerancji utraty danych, harmonogramu punktów odzyskiwania, a w przypadku aplikacji bazy danych — na podstawie harmonogramu ekspresowej pełnej kopii zapasowej.

Zakres przechowywania określa, jak długo ma być dostępna utworzona kopia zapasowa danych. Czy dzisiejsze dane mają być na przykład dostępne przez tydzień? Przez dwa tygodnie? Przez rok?

Tolerancja utraty danych to maksymalna ilość utraconych danych mierzona w jednostkach czasu, która jest zgodna z wymaganiami biznesowymi. Określa, jak często program DPM powinien synchronizować się z chronionym serwerem i zbierać z niego zmiany danych. Częstotliwość synchronizacji można dowolnie zmieniać — od 15 minut do 24 godzin. Można również określić, aby synchronizacja odbywała się chwilę przed utworzeniem punktu odzyskiwania, a nie w terminie określonym w harmonogramie.

Harmonogram punktów odzyskiwania określa, ile punktów odzyskiwania danych ma być tworzonych dla danej grupy ochrony. W przypadku ochrony plików wybiera się dni i godziny, w których mają być tworzone punkty odzyskiwania. W przypadku ochrony danych aplikacji obsługujących przyrostowe kopie zapasowe harmonogram punktów odzyskiwania zależy od częstotliwości synchronizacji. W przypadku ochrony danych aplikacji nieobsługujących przyrostowych kopii zapasowych harmonogram punktów odzyskiwania zależy od harmonogramu ekspresowej pełnej kopii zapasowej.

NOTE

Po utworzeniu grupy ochrony program DPM określa typ chronionych danych i umożliwia wybranie opcji ochrony dostępnych tylko w ramach tych danych.

Proces autowykrywania

Autowykrywanie jest codziennym procesem, za pomocą którego program DPM automatycznie wykrywa nowe komputery w sieci i te, które zostały z niej usunięte. Raz dziennie, w czasie, który można zaplanować, program DPM wysyła mały pakiet (mniej niż 10 kilobajtów) do najbliższego kontrolera domeny. Kontroler domeny odpowiada na żądanie protokołu LDAP z komputerów w tej domenie, a program DPM identyfikuje nowe i usunięte komputery. Ruch sieciowy tworzony przez proces autowykrywania jest minimalny.

Funkcja autowykrywania nie wykrywa nowych i usuniętych komputerów w innych domenach. Aby zainstalować agenta ochrony na komputerze w innej domenie, należy zidentyfikować komputer przy użyciu jego w pełni kwalifikowanej nazwy domeny.

Struktura katalogów programu DPM

Po rozpoczęciu ochrony danych przy użyciu programu DPM można zauważyć, że ścieżka instalacji programu DPM zawiera trzy foldery w katalogu Volumes:

- \Microsoft DPM\DPM\Volumes\DiffArea
- \Microsoft DPM\DPM\Volumes\Replica
- \Microsoft DPM\DPM\Volumes\ShadowCopy

Folder DiffArea zawiera zainstalowane woluminy kopii w tle, które przechowują punkty odzyskiwania źródła danych.

Folder Replica zawiera zainstalowane woluminy repliki danych.

Folder ShadowCopy zawiera lokalne kopie zapasowe bazy danych programu DPM. Jeśli program DPMBackup.exe jest używany w celu utworzenia kopii zapasowych w tle dla replik archiwum przy użyciu oprogramowania kopii zapasowej innych firm, kopie zapasowe w tle są przechowywane w folderze ShadowCopy.

Telemetria programu DPM

Program DPM nie zbiera żadnych danych telemetrycznych. W przypadku wysyłania danych do platformy Azure informacje potrzebne Azure Backup są wysyłane do firmy Microsoft. Nie zawiera żadnych danych OSOBOWYCH.

What can DPM back up? (Co program DPM może umieścić w kopii zapasowej?)

21.02.2020 • 35 minutes to read

Ten artykuł zawiera szczegółowe informacje o obciążeniach, których kopia zapasowa ma zostać utworzona w programie DPM.

W przypadku programu DPM 2016 i pół-roczne wersje kanału należy użyć następującej macierzy: 1801 i 1807:

- Obciążenia — typ obciążenia technologii.
- Wersja — obsługiwana wersja programu VMM dla obciążeń.
- Instalacja programu DPM — komputera/lokalizacji, w której chcesz zainstalować program DPM.
- Ochrona i odzyskiwanie — lista szczegółowych informacji o obciążeniach, takich jak obsługiwane kontenery magazynu lub obsługiwane wdrożenie.

Użyj poniższej macierzy dla programu DPM 2019:

- Obciążenia — typ obciążenia technologii.
- Wersja — obsługiwana wersja programu VMM dla obciążeń.
- Instalacja programu DPM — komputera/lokalizacji, w której chcesz zainstalować program DPM.
- Ochrona i odzyskiwanie — lista szczegółowych informacji o obciążeniach, takich jak obsługiwane kontenery magazynu lub obsługiwane wdrożenie.

Macierz obsługi ochrony

W poniższych sekcjach szczegółowo opisano Macierz obsługi ochrony programu DPM:

- [Tworzenie kopii zapasowej aplikacji](#)
- [Kopia zapasowa maszyny wirtualnej](#)
- [Linux](#)

Tworzenie kopii zapasowej aplikacji

OBCIĄŻENIE	WERSJA	INSTALACJA PROGRAMU DPM	OCHRONA I ODZYSKIWANIE
------------	--------	----------------------------	------------------------

OBCIĄŻENIE	WERSJA	INSTALACJA PROGRAMU DPM	OCHRONA I ODZYSKIWANIE
Komputery klienckie (64-bitowe)	Windows 10	Serwer fizyczny Maszyna wirtualna funkcji Hyper-V Maszyna wirtualna VMware	Wolumin, udział, folder, pliki, deduplikowane woluminy Chronione woluminy muszą mieć system plików NTFS. Systemy plików FAT i FAT32 nie są obsługiwane. Woluminy muszą mieć co najmniej 1 GB. Program DPM korzysta z usługi kopiowania woluminów w tle (VSS) do tworzenia migawek chronionych danych, a migawka zostanie utworzona tylko wtedy, gdy rozmiar woluminu będzie wynosił co najmniej 1 GB.
Serwery (64-bitowe)	Windows Server 2019, 2016, 2012 R2, 2012	Maszyna wirtualna platformy Azure (gdy obciążenie działa jako maszyna wirtualna platformy Azure) Maszyna wirtualna systemu Windows w środowisku programu VMWare (chroni obciążenia działające na maszynie wirtualnej systemu Windows w programie VMWare) Serwer fizyczny Lokalna maszyna wirtualna funkcji Hyper-V	Wolumin, udział, folder, plik, deduplikowane woluminy. Stan systemu i system bez systemu operacyjnego (nieobsługiwane dla maszyny wirtualnej platformy Azure). Program DPM 2019 UR1 obsługuje ochronę woluminów ReFS i woluminu z deduplikacją systemu plików ReFS.
Program System Center VMM	VMM 2019, 2016	Serwer fizyczny Maszyna wirtualna funkcji Hyper-V	Wszystkie scenariusze wdrażania: baza danych
Serwer SQL	SQL Server 2019, SQL Server 2017, 2016 i obsługiwane przez program sps, 2014 i obsługiwanego programu SPS	Serwer fizyczny Lokalna maszyna wirtualna funkcji Hyper-V Maszyna wirtualna platformy Azure Maszyna wirtualna systemu Windows w środowisku programu VMWare (chroni obciążenia działające na maszynie wirtualnej systemu Windows w programie VMWare)	Wszystkie scenariusze wdrażania: baza danych Program DPM 2019 UR1 obsługuje tworzenie kopii zapasowych bazy danych SQL w systemie plików ReFS

OBCIĄŻENIE	WERSJA	INSTALACJA PROGRAMU DPM	OCHRONA I ODZYSKIWANIE
Program Exchange	Exchange 2019, 2016	Serwer fizyczny Lokalna maszyna wirtualna funkcji Hyper-V	Ochrona (wszystkie scenariusze wdrażania): autonomiczny serwer programu Exchange, baza danych w grupie dostępności bazy danych (DAG) Odzyskiwanie (wszystkie scenariusze wdrażania): skrzynka pocztowa, bazy danych skrzynek pocztowych w grupie DAG Program DPM 2019 nie obsługuje tworzenia kopii zapasowych programu Exchange za pośrednictwem systemu plików ReFS. Program DPM 2019 UR1 obsługuje tworzenie kopii zapasowych programu Exchange za pośrednictwem systemu plików ReFS
SharePoint	SharePoint 2019, 2016 z najnowszymi programem SPs	Serwer fizyczny Lokalna maszyna wirtualna funkcji Hyper-V Maszyna wirtualna platformy Azure (gdy obciążenie działa jako maszyna wirtualna platformy Azure) Maszyna wirtualna systemu Windows w środowisku programu VMWare (chroni obciążenia działające na maszynie wirtualnej systemu Windows w programie VMWare)	Ochrona (wszystkie scenariusze wdrażania): farma, zawartość serwera frontonu sieci Web Odzyskiwanie (wszystkie scenariusze wdrażania): farma, baza danych, aplikacja internetowa, plik lub element listy, wyszukiwanie programu SharePoint, serwer frontonu internetowego Program DPM 2019 UR1 obsługuje tworzenie kopii zapasowych programu SharePoint w systemie plików ReFS

Kopia zapasowa maszyny wirtualnej

OBCIĄŻENIE	WERSJA	INSTALACJA PROGRAMU DPM	OCHRONA I ODZYSKIWANIE
------------	--------	-------------------------	------------------------

OBCIĄŻENIE	WERSJA	INSTALACJA PROGRAMU DPM	OCHRONA I ODZYSKIWANIE
Host funkcji Hyper-V — agent ochrony DPM na serwerze hosta, klastrze lub maszynie wirtualnej funkcji Hyper-V	Windows Server 2019, 2016, 2012 R2, 2012	Serwer fizyczny Lokalna maszyna wirtualna funkcji Hyper-V	Ochrona: komputery funkcji Hyper-V, maszyny wirtualne funkcji Hyper-V hostowane w systemie (udostępnione woluminy klastra) CSV Odzyskiwanie: maszyna wirtualna, odzyskiwanie plików i folderów na poziomie elementu, woluminy, wirtualne dyski twarde
Maszyny wirtualne VMware	Serwer VMware 6,0 lub 6,5, 6,7	Serwer fizyczny Lokalna maszyna wirtualna funkcji Hyper-V	Maszyny wirtualne VMware na woluminach udostępnionych klastra (CSV), NFS i SAN. Odzyskiwanie plików i folderów na poziomie elementu jest dostępne tylko dla systemu Windows. Oprogramowanie VMware oprogramowania vApps nie jest obsługiwane.

Linux

OBCIĄŻENIE	WERSJA	INSTALACJA PROGRAMU DPM	OCHRONA I ODZYSKIWANIE
Linux	System Linux uruchomiony jako gość funkcji Hyper-V (funkcja Hyper-V uruchomiona w systemie Windows Server 2016/2019/2012 R2/2012)	Lokalna maszyna wirtualna funkcji Hyper-V	Funkcja Hyper-V musi być uruchomiona w systemie Windows Server 2019, Windows Server 2016, Windows Server 2012 R2 lub Windows Server 2012. Ochrona: cała maszyna wirtualna Odzyskiwanie: cała maszyna wirtualna Obsługiwane są tylko migawki zgodne z plikami. Aby zapoznać się z pełną listą obsługiwanych dystrybucji systemu Linux i wersji, zapoznaj się z artykułem Linux na temat dystrybucji zatwierdzonym przez platformę Azure .

Macierz obsługi ochrony

OBCIĄŻENIE	WERSJA	INSTALACJA PROGRAMU DPM	PROGRAM DPM — KONSOLA SAC PROGRAMU SYSTEM CENTER	DPM — SYSTEM CENTER 2016	OCHRONA I ODZYSKIWANIE
Program System Center VMM	VMM 2016, VMM 2012, SP1, R2	Serwer fizyczny Maszyna wirtualna funkcji Hyper-V	T	T	Wszystkie scenariusze wdrażania: baza danych
Komputery klienckie (64-bitowe i 32-bitowe)	Windows 10	Serwer fizyczny Maszyna wirtualna funkcji Hyper-V Maszyna wirtualna VMware	T	T	Wolumin, udział, folder, pliki, deduplikowane woluminy Chronione woluminy muszą mieć system plików NTFS. Systemy plików FAT i FAT32 nie są obsługiwane. Woluminy muszą mieć co najmniej 1 GB. Program DPM korzysta z usługi kopiowania woluminów w tle (VSS) do tworzenia migawek chronionych danych, a migawka zostanie utworzona tylko wtedy, gdy rozmiar woluminu będzie wynosił co najmniej 1 GB.

OBCIĄŻENIE	WERSJA	INSTALACJA PROGRAMU DPM	PROGRAM DPM — KONSOLA SAC PROGRAMU SYSTEM CENTER	DPM — SYSTEM CENTER 2016	OCHRONA I ODZYSKIWANIE
Komputery klienckie (64-bitowe i 32-bitowe)	Windows 8.1	Serwer fizyczny Maszyna wirtualna funkcji Hyper-V	T	T	Wolumin, udział, folder, pliki, deduplikowane woluminy Chronione woluminy muszą mieć system plików NTFS. Systemy plików FAT i FAT32 nie są obsługiwane. Woluminy muszą mieć co najmniej 1 GB. Program DPM korzysta z usługi kopiowania woluminów w tle (VSS) do tworzenia migawek chronionych danych, a migawka zostanie utworzona tylko wtedy, gdy rozmiar woluminu będzie wynosił co najmniej 1 GB.

OBCIĄŻENIE	WERSJA	INSTALACJA PROGRAMU DPM	PROGRAM DPM — KONSOLA SAC PROGRAMU SYSTEM CENTER	DPM — SYSTEM CENTER 2016	OCHRONA I ODZYSKIWANIE
Komputery klienckie (64-bitowe i 32-bitowe)	Windows 8.1	Maszyna wirtualna systemu Windows w środowisku programu VMWare (chroni obciążenia działające na maszynie wirtualnej systemu Windows w programie VMWare)	T	T Od pakietu Update Rollup 5	Wolumin, udział, folder, pliki, deduplikowane woluminy Chronione woluminy muszą mieć system plików NTFS. Systemy plików FAT i FAT32 nie są obsługiwane. Woluminy muszą mieć co najmniej 1 GB. Program DPM korzysta z usługi kopiowania woluminów w tle (VSS) do tworzenia migawek chronionych danych, a migawka zostanie utworzona tylko wtedy, gdy rozmiar woluminu będzie wynosił co najmniej 1 GB.
Komputery klienckie (64-bitowe i 32-bitowe)	Windows 8	Serwer fizyczny Lokalna maszyna wirtualna funkcji Hyper-V	T	T	Wolumin, udział, folder, pliki, deduplikowane woluminy Chronione woluminy muszą mieć system plików NTFS i rozmiar co najmniej 1 GB.

OBCIĄŻENIE	WERSJA	INSTALACJA PROGRAMU DPM	PROGRAM DPM — KONSOLA SAC PROGRAMU SYSTEM CENTER	DPM — SYSTEM CENTER 2016	OCHRONA I ODZYSKIWANIE
Komputery klienckie (64-bitowe i 32-bitowe)	Windows 8	Maszyna wirtualna systemu Windows w środowisku programu VMWare (chroni obciążenia działające na maszynie wirtualnej systemu Windows w programie VMWare)	T	T	Wolumin, udział, folder, pliki, deduplikowane woluminy Chronione woluminy muszą mieć system plików NTFS. Systemy plików FAT i FAT32 nie są obsługiwane. Woluminy muszą mieć co najmniej 1 GB. Program DPM korzysta z usługi kopiowania woluminów w tle (VSS) do tworzenia migawek chronionych danych, a migawka zostanie utworzona tylko wtedy, gdy rozmiar woluminu będzie wynosił co najmniej 1 GB.
Komputery klienckie (64-bitowe i 32-bitowe)	Windows 7	Serwer fizyczny Lokalna maszyna wirtualna funkcji Hyper-V	T	T	Wolumin, udział, folder, pliki, deduplikowane woluminy Chronione woluminy muszą mieć system plików NTFS i rozmiar co najmniej 1 GB.

OBCIĄŻENIE	WERSJA	INSTALACJA PROGRAMU DPM	PROGRAM DPM — KONSOLA SAC PROGRAMU SYSTEM CENTER	DPM — SYSTEM CENTER 2016	OCHRONA I ODZYSKIWANIE
Komputery klienckie (64-bitowe i 32-bitowe)	Windows 7	Maszyna wirtualna systemu Windows w środowisku programu VMWare (chroni obciążenia działające na maszynie wirtualnej systemu Windows w programie VMWare)	T	T	Wolumin, udział, folder, pliki, deduplikowane woluminy Chronione woluminy muszą mieć system plików NTFS. Systemy plików FAT i FAT32 nie są obsługiwane. Woluminy muszą mieć co najmniej 1 GB. Program DPM korzysta z usługi kopiowania woluminów w tle (VSS) do tworzenia migawek chronionych danych, a migawka zostanie utworzona tylko wtedy, gdy rozmiar woluminu będzie wynosił co najmniej 1 GB.

OBCIĄŻENIE	WERSJA	INSTALACJA PROGRAMU DPM	PROGRAM DPM — KONSOLA SAC PROGRAMU SYSTEM CENTER	DPM — SYSTEM CENTER 2016	OCHRONA I ODZYSKIWANIE
Serwery (32-bitowe i 64-bitowe)	Windows Server 2016	Maszyna wirtualna platformy Azure (gdy obciążenie działa jako maszyna wirtualna platformy Azure) Maszyna wirtualna systemu Windows w środowisku programu VMWare (chroni obciążenia działające na maszynie wirtualnej systemu Windows w programie VMWare) Serwer fizyczny Lokalna maszyna wirtualna funkcji Hyper-V	T Nie serwer Nano	T Nie serwer Nano	Wolumin, udział, folder, plik, stan systemu/bez systemu operacyjnego, deduplikowane woluminy
Serwery (32-bitowe i 64-bitowe)	Windows Server 2012 R2 — wersja Datacenter i Standard	Maszyna wirtualna platformy Azure (gdy obciążenie działa jako maszyna wirtualna platformy Azure)	T	T	Wolumin, udział, folder, plik Aby chronić woluminy z deduplikacją systemu Windows Server 2012, program DPM musi działać co najmniej w systemie Windows Server 2012 R2.

OBCIĄŻENIE	WERSJA	INSTALACJA PROGRAMU DPM	PROGRAM DPM — KONSOLA SAC PROGRAMU SYSTEM CENTER	DPM — SYSTEM CENTER 2016	OCHRONA I ODZYSKIWANIE
Serwery (32-bitowe i 64-bitowe)	Windows Server 2012 R2 — wersja Datacenter i Standard	Maszyna wirtualna systemu Windows w środowisku programu VMWare (chroni obciążenia działające na maszynie wirtualnej systemu Windows w programie VMWare)	T	T	Wolumin, udział, folder, plik, stan systemu/bez systemu operacyjnego Aby chronić woluminy z deduplikacją systemu Windows Server 2012, program DPM musi działać w systemie Windows Server 2012 lub Windows Server 2012 R2.
Serwery (32-bitowe i 64-bitowe)	Windows Server 2012/2012 z dodatkiem SP1 — wersja Datacenter i Standard	Serwer fizyczny Lokalna maszyna wirtualna funkcji Hyper-V	T	T	Wolumin, udział, folder, plik, stan systemu/bez systemu operacyjnego Aby chronić woluminy z deduplikacją systemu Windows Server 2012, program DPM musi działać co najmniej w systemie Windows Server 2012 R2.
Serwery (32-bitowe i 64-bitowe)	Windows Server 2012/2012 z dodatkiem SP1 — wersja Datacenter i Standard	Maszyna wirtualna platformy Azure (gdy obciążenie działa jako maszyna wirtualna platformy Azure)	T	T	Wolumin, udział, folder, plik Aby chronić woluminy z deduplikacją systemu Windows Server 2012, program DPM musi działać co najmniej w systemie Windows Server 2012 R2.

OBCIĄŻENIE	WERSJA	INSTALACJA PROGRAMU DPM	PROGRAM DPM — KONSOLA SAC PROGRAMU SYSTEM CENTER	DPM — SYSTEM CENTER 2016	OCHRONA I ODZYSKIWANIE
Serwery (32-bitowe i 64-bitowe)	Windows Server 2012/2012 z dodatkiem SP1 — wersja Datacenter i Standard	Maszyna wirtualna systemu Windows w środowisku programu VMWare (chroni obciążenia działające na maszynie wirtualnej systemu Windows w programie VMWare)	T	T	Wolumin, udział, folder, plik, stan systemu/bez systemu operacyjnego Aby chronić woluminy z deduplikacją systemu Windows Server 2012, program DPM musi działać co najmniej w systemie Windows Server 2012 R2.
Serwery (32-bitowe i 64-bitowe)	Windows Server 2008 R2 z dodatkiem SP1 — wersja Standard i Enterprise	Serwer fizyczny Lokalna maszyna wirtualna funkcji Hyper-V	T Musisz korzystać z dodatku SP1 i mieć zainstalowane oprogramowanie Windows Management Frame 4.0	T Należy zainstalować ramkę zarządzania systemu Windows 4,0	Wolumin, udział, folder, plik, stan systemu/bez systemu operacyjnego
Serwery (32-bitowe i 64-bitowe)	Windows Server 2008 R2 z dodatkiem SP1 — wersja Standard i Enterprise	Maszyna wirtualna platformy Azure (gdy obciążenie działa jako maszyna wirtualna platformy Azure)	T Należy zainstalować ramkę zarządzania systemu Windows 4,0	T Musisz korzystać z dodatku SP1 i mieć zainstalowane oprogramowanie Windows Management Frame 4.0	Wolumin, udział, folder, plik
Serwery (32-bitowe i 64-bitowe)	Windows Server 2008 R2 z dodatkiem SP1 — wersja Standard i Enterprise	Maszyna wirtualna systemu Windows w środowisku programu VMWare (chroni obciążenia działające na maszynie wirtualnej systemu Windows w programie VMWare)	T Należy zainstalować ramkę zarządzania systemu Windows 4,0	T Musisz korzystać z dodatku SP1 i mieć zainstalowane oprogramowanie Windows Management Frame 4.0	Wolumin, udział, folder, plik, stan systemu/bez systemu operacyjnego

OBCIĄŻENIE	WERSJA	INSTALACJA PROGRAMU DPM	PROGRAM DPM — KONSOLA SAC PROGRAMU SYSTEM CENTER	DPM — SYSTEM CENTER 2016	OCHRONA I ODZYSKIWANIE
Serwery (32-bitowe i 64-bitowe)	Windows Server 2008 R2	Serwer fizyczny Lokalna maszyna wirtualna funkcji Hyper-V	T	T	Wolumin, udział, folder, plik, stan systemu/bez systemu operacyjnego
Serwery (32-bitowe i 64-bitowe)	Windows Server 2008 R2	Maszyna wirtualna platformy Azure (gdy obciążenie działa jako maszyna wirtualna platformy Azure)	N	N	Wolumin, udział, folder, plik
Serwery (32-bitowe i 64-bitowe)	Windows Server 2008 R2	Maszyna wirtualna systemu Windows w środowisku programu VMWare (chroni obciążenia działające na maszynie wirtualnej systemu Windows w programie VMWare)	N	N	Wolumin, udział, folder, plik, stan systemu/bez systemu operacyjnego
Serwery (32-bitowe i 64-bitowe)	Windows Server 2008 SP2	Serwer fizyczny Lokalna maszyna wirtualna funkcji Hyper-V	N	N	Wolumin, udział, folder, plik, stan systemu/bez systemu operacyjnego
Serwery (32-bitowe i 64-bitowe)	Windows Server 2008 SP2	Maszyna wirtualna systemu Windows w środowisku programu VMWare (chroni obciążenia działające na maszynie wirtualnej systemu Windows w programie VMWare)	T	T	Wolumin, udział, folder, plik, stan systemu/bez systemu operacyjnego

OBCIĄŻENIE	WERSJA	INSTALACJA PROGRAMU DPM	PROGRAM DPM — KONSOLA SAC PROGRAMU SYSTEM CENTER	DPM — SYSTEM CENTER 2016	OCHRONA I ODZYSKIWANIE
Serwery (32-bitowe i 64-bitowe)	Windows Storage Server 2008 z dodatkiem SP2	Serwer fizyczny Lokalna maszyna wirtualna funkcji Hyper-V	T	T	Wolumin, udział, folder, plik, stan systemu/bez systemu operacyjnego
Serwer SQL	SQL Server 2017	Serwer fizyczny Lokalna maszyna wirtualna funkcji Hyper-V Maszyna wirtualna platformy Azure Maszyna wirtualna systemu Windows w środowisku programu VMWare (chroni obciążenia działające na maszynie wirtualnej systemu Windows w programie VMWare)	T	T (UR5 lub nowszy)	Wszystkie scenariusze wdrażania: baza danych
Serwer SQL	SQL Server 2016 SP1	Serwer fizyczny Lokalna maszyna wirtualna funkcji Hyper-V Maszyna wirtualna platformy Azure Maszyna wirtualna systemu Windows w środowisku programu VMWare (chroni obciążenia działające na maszynie wirtualnej systemu Windows w programie VMWare)	T	T (UR4 lub nowszy)	Wszystkie scenariusze wdrażania: baza danych

OBCIĄŻENIE	WERSJA	INSTALACJA PROGRAMU DPM	PROGRAM DPM — KONSOLA SAC PROGRAMU SYSTEM CENTER	DPM — SYSTEM CENTER 2016	OCHRONA I ODZYSKIWANIE
Serwer SQL	SQL Server 2016	Serwer fizyczny Lokalna maszyna wirtualna funkcji Hyper-V Maszyna wirtualna platformy Azure Maszyna wirtualna systemu Windows w środowisku programu VMWare (chroni obciążenia działające na maszynie wirtualnej systemu Windows w programie VMWare)	T	T (pakiet UR2 lub nowszy)	Wszystkie scenariusze wdrażania: baza danych
Serwer SQL	SQL Server 2014	Maszyna wirtualna platformy Azure (gdy obciążenie działa jako maszyna wirtualna platformy Azure)	T	T	Wszystkie scenariusze wdrażania: baza danych
Serwer SQL	SQL Server 2014	Maszyna wirtualna systemu Windows w środowisku programu VMWare (chroni obciążenia działające na maszynie wirtualnej systemu Windows w programie VMWare)	T	T	Wszystkie scenariusze wdrażania: baza danych
Serwer SQL	SQL Server 2012 z dodatkiem SP2	Serwer fizyczny Lokalna maszyna wirtualna funkcji Hyper-V	T	T	Wszystkie scenariusze wdrażania: baza danych

OBCIĄŻENIE	WERSJA	INSTALACJA PROGRAMU DPM	PROGRAM DPM — KONSOLA SAC PROGRAMU SYSTEM CENTER	DPM — SYSTEM CENTER 2016	OCHRONA I ODZYSKIWANIE
Serwer SQL	SQL Server 2012 z dodatkiem SP2	Maszyna wirtualna platformy Azure (gdy obciążenie działa jako maszyna wirtualna platformy Azure)	T	T	Wszystkie scenariusze wdrażania: baza danych
Serwer SQL	SQL Server 2012 z dodatkiem SP2	Maszyna wirtualna systemu Windows w środowisku programu VMWare (chroni obciążenia działające na maszynie wirtualnej systemu Windows w programie VMWare)	T	T	Wszystkie scenariusze wdrażania: baza danych
Serwer SQL	SQL Server 2012, SQL Server 2012 z dodatkiem SP1	Serwer fizyczny Lokalna maszyna wirtualna funkcji Hyper-V	T	T	Wszystkie scenariusze wdrażania: baza danych
Serwer SQL	SQL Server 2012, SQL Server 2012 z dodatkiem SP1	Maszyna wirtualna platformy Azure (gdy obciążenie działa jako maszyna wirtualna platformy Azure)	T	T	Wszystkie scenariusze wdrażania: baza danych
Serwer SQL	SQL Server 2012, SQL Server 2012 z dodatkiem SP1	Maszyna wirtualna systemu Windows w środowisku programu VMWare (chroni obciążenia działające na maszynie wirtualnej systemu Windows w programie VMWare)	T	T	Wszystkie scenariusze wdrażania: baza danych

OBCIĄŻENIE	WERSJA	INSTALACJA PROGRAMU DPM	PROGRAM DPM — KONSOLA SAC PROGRAMU SYSTEM CENTER	DPM — SYSTEM CENTER 2016	OCHRONA I ODZYSKIWANIE
Serwer SQL	SQL Server 2008 R2	Serwer fizyczny Lokalna maszyna wirtualna funkcji Hyper-V	T	T	Wszystkie scenariusze wdrażania: baza danych
Serwer SQL	SQL Server 2008 R2	Maszyna wirtualna platformy Azure (gdy obciążenie działa jako maszyna wirtualna platformy Azure)	T	T	Wszystkie scenariusze wdrażania: baza danych
Serwer SQL	SQL Server 2008 R2	Maszyna wirtualna systemu Windows w środowisku programu VMWare (chroni obciążenia działające na maszynie wirtualnej systemu Windows w programie VMWare)	T	T	Wszystkie scenariusze wdrażania: baza danych
Serwer SQL	SQL Server 2008	Serwer fizyczny Lokalna maszyna wirtualna funkcji Hyper-V	T	T	Wszystkie scenariusze wdrażania: baza danych
Serwer SQL	SQL Server 2008	Maszyna wirtualna platformy Azure (gdy obciążenie działa jako maszyna wirtualna platformy Azure)	T	T	Wszystkie scenariusze wdrażania: baza danych

OBCIĄŻENIE	WERSJA	INSTALACJA PROGRAMU DPM	PROGRAM DPM — KONSOLA SAC PROGRAMU SYSTEM CENTER	DPM — SYSTEM CENTER 2016	OCHRONA I ODZYSKIWANIE
Serwer SQL	SQL Server 2008	Maszyna wirtualna systemu Windows w środowisku programu VMWare (chroni obciążenia działające na maszynie wirtualnej systemu Windows w programie VMWare)	T	T	Wszystkie scenariusze wdrażania: baza danych
Program Exchange	Exchange 2016	Serwer fizyczny Lokalna maszyna wirtualna funkcji Hyper-V	T	T	Ochrona (wszystkie scenariusze wdrażania): autonomiczny serwer programu Exchange, baza danych w grupie dostępności bazy danych (DAG) Odzyskiwanie (wszystkie scenariusze wdrażania): skrzynka pocztowa, bazy danych skrzynek pocztowych w grupie DAG Tworzenie kopii zapasowej programu Exchange przy użyciu systemu plików ReFS nie jest obsługiwane

OBCIĄŻENIE	WERSJA	INSTALACJA PROGRAMU DPM	PROGRAM DPM — KONSOLA SAC PROGRAMU SYSTEM CENTER	DPM — SYSTEM CENTER 2016	OCHRONA I ODZYSKIWANIE
Program Exchange	Exchange 2016	Maszyna wirtualna systemu Windows w środowisku programu VMWare (chroni obciążenia działające na maszynie wirtualnej systemu Windows w programie VMWare)	T	T	Ochrona (wszystkie scenariusze wdrażania): autonomiczny serwer programu Exchange, baza danych w grupie dostępności bazy danych (DAG) Odzyskiwanie (wszystkie scenariusze wdrażania): skrzynka pocztowa, bazy danych skrzynek pocztowych w grupie DAG Tworzenie kopii zapasowej programu Exchange przy użyciu systemu plików ReFS nie jest obsługiwane

OBCIĄŻENIE	WERSJA	INSTALACJA PROGRAMU DPM	PROGRAM DPM — KONSOLA SAC PROGRAMU SYSTEM CENTER	DPM — SYSTEM CENTER 2016	OCHRONA I ODZYSKIWANIE
Program Exchange	Exchange 2013	Serwer fizyczny Lokalna maszyna wirtualna funkcji Hyper-V	T	T	Ochrona (wszystkie scenariusze wdrażania): autonomiczny serwer programu Exchange, baza danych w grupie dostępności bazy danych (DAG) Odzyskiwanie (wszystkie scenariusze wdrażania): skrzynka pocztowa, bazy danych skrzynek pocztowych w grupie DAG Tworzenie kopii zapasowej programu Exchange przy użyciu systemu plików ReFS nie jest obsługiwane

OBCIĄŻENIE	WERSJA	INSTALACJA PROGRAMU DPM	PROGRAM DPM — KONSOLA SAC PROGRAMU SYSTEM CENTER	DPM — SYSTEM CENTER 2016	OCHRONA I ODZYSKIWANIE
Program Exchange	Exchange 2013	Maszyna wirtualna systemu Windows w środowisku programu VMWare (chroni obciążenia działające na maszynie wirtualnej systemu Windows w programie VMWare)	T	T	Ochrona (wszystkie scenariusze wdrażania): autonomiczny serwer programu Exchange, baza danych w grupie dostępności bazy danych (DAG) Odzyskiwanie (wszystkie scenariusze wdrażania): skrzynka pocztowa, bazy danych skrzynek pocztowych w grupie DAG Tworzenie kopii zapasowej programu Exchange przy użyciu systemu plików ReFS nie jest obsługiwane

OBCIĄŻENIE	WERSJA	INSTALACJA PROGRAMU DPM	PROGRAM DPM — KONSOLA SAC PROGRAMU SYSTEM CENTER	DPM — SYSTEM CENTER 2016	OCHRONA I ODZYSKIWANIE
Program Exchange	Exchange 2010	Serwer fizyczny Lokalna maszyna wirtualna funkcji Hyper-V	T	T	Ochrona (wszystkie scenariusze wdrażania): autonomiczny serwer programu Exchange, baza danych w grupie dostępności bazy danych (DAG) Odzyskiwanie (wszystkie scenariusze wdrażania): skrzynka pocztowa, bazy danych skrzynek pocztowych w grupie DAG Tworzenie kopii zapasowej programu Exchange przy użyciu systemu plików ReFS nie jest obsługiwane

OBCIĄŻENIE	WERSJA	INSTALACJA PROGRAMU DPM	PROGRAM DPM — KONSOLA SAC PROGRAMU SYSTEM CENTER	DPM — SYSTEM CENTER 2016	OCHRONA I ODZYSKIWANIE
Program Exchange	Exchange 2010	Maszyna wirtualna systemu Windows w środowisku programu VMWare (chroni obciążenia działające na maszynie wirtualnej systemu Windows w programie VMWare)	T	T	Ochrona (wszystkie scenariusze wdrażania): autonomiczny serwer programu Exchange, baza danych w grupie dostępności bazy danych (DAG) Odzyskiwanie (wszystkie scenariusze wdrażania): skrzynka pocztowa, bazy danych skrzynek pocztowych w grupie DAG Tworzenie kopii zapasowej programu Exchange przy użyciu systemu plików ReFS nie jest obsługiwane

OBCIĄŻENIE	WERSJA	INSTALACJA PROGRAMU DPM	PROGRAM DPM — KONSOLA SAC PROGRAMU SYSTEM CENTER	DPM — SYSTEM CENTER 2016	OCHRONA I ODZYSKIWANIE
SharePoint	SharePoint 2016	Serwer fizyczny Lokalna maszyna wirtualna funkcji Hyper-V Maszyna wirtualna platformy Azure (gdy obciążenie działa jako maszyna wirtualna platformy Azure) Maszyna wirtualna systemu Windows w środowisku programu VMWare (chroni obciążenia działające na maszynie wirtualnej systemu Windows w programie VMWare)	T	T (pakiet UR2 lub nowszy)	Ochrona (wszystkie scenariusze wdrażania): farma, zawartość serwera frontonu sieci Web Odzyskiwanie (wszystkie scenariusze wdrażania): farma, baza danych, aplikacja internetowa, plik lub element listy, wyszukiwanie programu SharePoint, serwer frontonu internetowego
SharePoint	SharePoint 2013	Serwer fizyczny Lokalna maszyna wirtualna funkcji Hyper-V	T	T	Ochrona (wszystkie scenariusze wdrażania): farma, zawartość serwera frontonu sieci Web Odzyskiwanie (wszystkie scenariusze wdrażania): farma, baza danych, aplikacja internetowa, plik lub element listy, wyszukiwanie programu SharePoint, serwer frontonu internetowego

OBCIĄŻENIE	WERSJA	INSTALACJA PROGRAMU DPM	PROGRAM DPM — KONSOLA SAC PROGRAMU SYSTEM CENTER	DPM — SYSTEM CENTER 2016	OCHRONA I ODZYSKIWANIE
SharePoint	SharePoint 2013	Maszyna wirtualna platformy Azure (gdy obciążenie działa jako maszyna wirtualna platformy Azure) — od wersji DPM 2012 R2 z pakietem Update Rollup 3	T	T	Ochrona (wszystkie scenariusze wdrażania): farma, wyszukiwanie programu SharePoint, zawartość serwera frontonu sieci Web Odzyskiwanie (wszystkie scenariusze wdrażania): farma, baza danych, aplikacja internetowa, plik lub element listy, wyszukiwanie programu SharePoint, serwer frontonu internetowego
SharePoint	SharePoint 2013	Maszyna wirtualna systemu Windows w środowisku programu VMWare (chroni obciążenia działające na maszynie wirtualnej systemu Windows w programie VMWare)	T	T	Ochrona (wszystkie scenariusze wdrażania): farma, wyszukiwanie programu SharePoint, zawartość serwera frontonu sieci Web Odzyskiwanie (wszystkie scenariusze wdrażania): farma, baza danych, aplikacja internetowa, plik lub element listy, wyszukiwanie programu SharePoint, serwer frontonu internetowego

OBCIĄŻENIE	WERSJA	INSTALACJA PROGRAMU DPM	PROGRAM DPM — KONSOLA SAC PROGRAMU SYSTEM CENTER	DPM — SYSTEM CENTER 2016	OCHRONA I ODZYSKIWANIE
SharePoint	SharePoint 2010	Serwer fizyczny Lokalna maszyna wirtualna funkcji Hyper-V	T	T	Ochrona (wszystkie scenariusze wdrażania): farma, wyszukiwanie programu SharePoint, zawartość serwera frontonu sieci Web Odzyskiwanie (wszystkie scenariusze wdrażania): farma, baza danych, aplikacja internetowa, plik lub element listy, wyszukiwanie programu SharePoint, serwer frontonu internetowego
SharePoint	SharePoint 2010	Maszyna wirtualna platformy Azure (gdy obciążenie działa jako maszyna wirtualna platformy Azure)	T	T	Ochrona (wszystkie scenariusze wdrażania): farma, wyszukiwanie programu SharePoint, zawartość serwera frontonu sieci Web Odzyskiwanie (wszystkie scenariusze wdrażania): farma, baza danych, aplikacja internetowa, plik lub element listy, wyszukiwanie programu SharePoint, serwer frontonu internetowego

OBCIĄŻENIE	WERSJA	INSTALACJA PROGRAMU DPM	PROGRAM DPM — KONSOLA SAC PROGRAMU SYSTEM CENTER	DPM — SYSTEM CENTER 2016	OCHRONA I ODZYSKIWANIE
SharePoint	SharePoint 2010	Maszyna wirtualna systemu Windows w środowisku programu VMWare (chroni obciążenia działające na maszynie wirtualnej systemu Windows w programie VMWare)	T	T	Ochrona (wszystkie scenariusze wdrażania): farma, wyszukiwanie programu SharePoint, zawartość serwera frontonu sieci Web Odzyskiwanie (wszystkie scenariusze wdrażania): farma, baza danych, aplikacja internetowa, plik lub element listy, wyszukiwanie programu SharePoint, serwer frontonu internetowego
Host funkcji Hyper-V — agent ochrony DPM na serwerze hosta, klastrze lub maszynie wirtualnej funkcji Hyper-V	Windows Server 2016	Serwer fizyczny Lokalna maszyna wirtualna funkcji Hyper-V	T	T	Ochrona: komputery funkcji Hyper-V, maszyny wirtualne funkcji Hyper-V hostowane w systemie (udostępnione woluminy klastra) CSV Odzyskiwanie: maszyna wirtualna, odzyskiwanie plików i folderów na poziomie elementu, woluminy, wirtualne dyski twarde

OBCIĄŻENIE	WERSJA	INSTALACJA PROGRAMU DPM	PROGRAM DPM — KONSOLA SAC PROGRAMU SYSTEM CENTER	DPM — SYSTEM CENTER 2016	OCHRONA I ODZYSKIWANIE
Host funkcji Hyper-V — agent ochrony DPM na serwerze hosta, klastrze lub maszynie wirtualnej funkcji Hyper-V	Windows Server 2012 R2 — wersja Datacenter i Standard	Serwer fizyczny Lokalna maszyna wirtualna funkcji Hyper-V	T	T	Ochrona: komputery funkcji Hyper-V, maszyny wirtualne funkcji Hyper-V hostowane w systemie (udostępnione woluminy klastra) CSV Odzyskiwanie: maszyna wirtualna, odzyskiwanie plików i folderów na poziomie elementu, woluminy, wirtualne dyski twarde
Host funkcji Hyper-V — agent ochrony DPM na serwerze hosta, klastrze lub maszynie wirtualnej funkcji Hyper-V	Windows Server 2012 — wersja Datacenter i Standard	Serwer fizyczny Lokalna maszyna wirtualna funkcji Hyper-V	T	T	Ochrona: komputery funkcji Hyper-V, maszyny wirtualne funkcji Hyper-V hostowane w systemie (udostępnione woluminy klastra) CSV Odzyskiwanie: maszyna wirtualna, odzyskiwanie plików i folderów na poziomie elementu, woluminy, wirtualne dyski twarde

OBCIĄŻENIE	WERSJA	INSTALACJA PROGRAMU DPM	PROGRAM DPM — KONSOLA SAC PROGRAMU SYSTEM CENTER	DPM — SYSTEM CENTER 2016	OCHRONA I ODZYSKIWANIE
Host funkcji Hyper-V — agent ochrony DPM na serwerze hosta, klastrze lub maszynie wirtualnej funkcji Hyper-V	Windows Server 2008 R2 z dodatkiem SP1 — wersja Enterprise i Standard	Serwer fizyczny Lokalna maszyna wirtualna funkcji Hyper-V	T	T	Ochrona: komputery funkcji Hyper-V, maszyny wirtualne funkcji Hyper-V hostowane w systemie (udostępnione woluminy klastra) CSV Odzyskiwanie: maszyna wirtualna, odzyskiwanie plików i folderów na poziomie elementu, woluminy, wirtualne dyski twarde
Host funkcji Hyper-V — agent ochrony DPM na serwerze hosta, klastrze lub maszynie wirtualnej funkcji Hyper-V	Windows Server 2008 SP2	Serwer fizyczny Lokalna maszyna wirtualna funkcji Hyper-V	N	N	Ochrona: komputery funkcji Hyper-V, maszyny wirtualne funkcji Hyper-V hostowane w systemie (udostępnione woluminy klastra) CSV Odzyskiwanie: maszyna wirtualna, odzyskiwanie plików i folderów na poziomie elementu, woluminy, wirtualne dyski twarde

OBCIĄŻENIE	WERSJA	INSTALACJA PROGRAMU DPM	PROGRAM DPM — KONSOLA SAC PROGRAMU SYSTEM CENTER	DPM — SYSTEM CENTER 2016	OCHRONA I ODZYSKIWANIE
Linux	System Linux uruchomiony jako gość funkcji Hyper-V	Lokalna maszyna wirtualna funkcji Hyper-V	T	T	Funkcja Hyper-V musi być uruchomiona w systemie Windows Server 2012 R2 lub Windows Server 2016. Ochrona: cała maszyna wirtualna Odzyskiwanie: cała maszyna wirtualna Aby zapoznać się z pełną listą obsługiwanych dystrybucji systemu Linux i wersji, zapoznaj się z artykułem Linux na temat dystrybucji zatwierdzonym przez platformę Azure.
Maszyny wirtualne VMware	Oprogramowanie VMware Server 5,5, 6,0 lub 6,5	Lokalna maszyna wirtualna funkcji Hyper-V	T	N	Maszyny wirtualne VMware na woluminach udostępnionych klastrze (CSV), NFS i SAN. Odzyskiwanie plików i folderów na poziomie elementu jest dostępne tylko dla systemu Windows. Oprogramowanie VMware oprogramowania vApps nie jest obsługiwane.

OBCIĄŻENIE	WERSJA	INSTALACJA PROGRAMU DPM	PROGRAM DPM — KONSOLA SAC PROGRAMU SYSTEM CENTER	DPM — SYSTEM CENTER 2016	OCHRONA I ODZYSKIWANIE
Maszyny wirtualne VMware	VMware vSphere 6,7	Lokalna maszyna wirtualna funkcji Hyper-V	T (dotyczy programu DPM 1807 i nowszych)	N	Maszyny wirtualne VMware na woluminach udostępnionych klastra (CSV), NFS i SAN. Odzyskiwanie plików i folderów na poziomie elementu jest dostępne tylko dla systemu Windows. Oprogramowanie VMware oprogramowania vApps nie jest obsługiwane.

Obsługa klastrów

Program DPM może chronić dane w następujących aplikacjach klastrowanych:

- Serwery plików
- Serwer SQL
- Funkcja Hyper-V

NOTE

W przypadku ochrony klastra funkcji Hyper-V przy użyciu skalowanej ochrony programu DPM nie można dodać dodatkowej ochrony dla chronionych obciążeń funkcji Hyper-V.

- Program Exchange Server — program DPM może chronić nieudostępniane klastry dysków z obsługiwanymi wersjami programu Exchange Server (ciągła replikacja klastra) oraz program Exchange Server skonfigurowany do lokalnej replikacji ciągłej.
- Serwer SQL

NOTE

Program DPM nie obsługuje ochrony baz danych SQL Server hostowanych na udostępnionych woluminach klastra (CSV).

Przy użyciu programu DPM można chronić obciążenia klastrów w tej samej domenie, w której znajduje się serwer programu DPM, albo w domenie podrzędnej lub zaufanej. Jeśli chcesz chronić źródło danych w niezaufanych domenach lub grupach roboczych, zastosuj uwierzytelnianie przy użyciu protokołu NTLM lub certyfikatu dla jednego serwera albo uwierzytelnianie tylko przy użyciu certyfikatu dla klastra.

Następne kroki

Biblioteki taśm zgodne z programem System Center DPM

11.12.2019 • 39 minutes to read

Data Protection Manager (DPM) w programie System Center 2012 R2, 2016 i 2019 można wdrożyć przy użyciu kopii zapasowej opartej na taśmach dla danych chronionych przez serwer programu DPM. Biblioteka taśm lub autonomiczna stacja taśm może być podłączona do serwerów programu DPM. Aby uzyskać więcej informacji, zobacz [Planowanie konfiguracji bibliotek taśm](#). Poniższe tabele zawierają podsumowanie bibliotek taśm zgodnych z programem DPM w programie System Center 2012 R2, 2016 i 2019.

NOTE

Biblioteki taśm skonfigurowane za pomocą wirtualnej karty protokołu Fibre Channel są obsługiwane tylko w przypadku korzystania ze sprzętu z certyfikowaną biblioteką taśm w następujących konfiguracjach:

- System Center Data Protection Manager 2012 R2 U3 (lub nowszy) działający w systemie Windows 2012 R2 (lub nowszym).
- Program System Center Data Protection Manager 2016 działający w systemie Windows Server 2012 R2 (lub nowszym).
- Program System Center Data Protection Manager 2019 działający w systemach Windows Server 2016 i Windows Server 2019.

Macierz obsługi

	DPM 2012 R2	DPM 2016	DPM 2019
Windows Server 2012 R2	T	T	N
Windows Server 2016	T	T	T
Windows Server 2019	N	N	T

BDT

NAZWA MODELU BIBLIOTEKI	SYSTEM OPERACYJNY	WERSJA STEROWNIKA ZMIENIACZA	WERSJA OPROGRAMOWANIA UKŁADOWEGO BIBLIOTEKI	DODATKOWE BIBLIOTEKI W TEŚCIE	TYP STACJI TAŚM	WERSJA STEROWNIKA TAŚMY	WERSJA OPROGRAMOWANIA UKŁADOWEGO STACJI TAŚM
FlexStor II 1U		5.2.3790.7, 06/06/2009, podpisane	2.4	2U, 4U, 8U	HP LTO5 HH FC	1.0.6.3, 10/07/2010, podpisane	Y23B
FlexStor II 1U		5.2.3790.7, 06/06/2009, podpisane	2.4	2U, 4U, 8U	HP LTO5 HH SAS	1.0.6.3, 10/07/2010, podpisane	Z21B

NAZWA MODELU BIBLIOTEKI	SYSTEM OPERACYJNY	WERSJA STEROWNIK A ZMIENIACZA	WERSJA OPROGRAM OWANIA UKŁADOWE GO BIBLIOTEKI	DODATKOW E BIBLIOTEKI W TEŚCIE	TYP STACJI TAŚM	WERSJA STEROWNIK A TAŚMY	WERSJA OPROGRAM OWANIA UKŁADOWE GO STACJI TAŚM
FlexStor II — 4U		5.2.3790.7, 06/06/2009 , podpisane	4.70/3,00 e	2U, 8U	SAS HP LTO5 FH	1.0.6.1, 05/14/2009 , podpisane	X22B
FlexStor II — 4U		5.2.3790.7, 06/06/2009 , podpisane	4.70/3,00 e	2U, 8U	HP LTO5 FH FC	1.0.6.3, 10/07/2010 , podpisane	I5BB
FlexStor II — 4U		5.2.3790.7, 06/06/2009 , podpisane	4.70/3,00 e	2U, 8U	IBM LTO5 FH FC	6.2.1.5, 01/13/2011 , podpisane	A6S0
FlexStor II — 4U		5.2.3790.7, 06/06/2009 , podpisane	4.70/3,00 e	2U, 8U	SAS IBM LTO5 FH	6.2.1.5, 01/13/2011 , podpisane	A6S0
FlexStor II — 4U		5.2.3790.7, 06/06/2009 , podpisane	4.70/3,00 e	1U, 2U, 8U	IBM LTO5 HH FC	6.2.1.5, 01/13/2011 , podpisane	A6S1
FlexStor II — 4U		5.2.3790.7, 06/06/2009 , podpisane	4.70/3,00 e	1U, 2U, 8U	IBM LTO5 HH SAS	6.2.1.5, 01/13/2011 , podpisane	A6S1
FlexStor II — 4U	2008 R2	5.2.3790.7, 06/06/2009 , podpisane	4.90/3.20 e	1U, 2U, 8U	HP LTO6 HH FC	1.0.7.1, 02/11/2013 , podpisane	22EB
FlexStor II — 4U	2012	8.0.0.1, 07/05/2012 , podpisane	4.90/3.20 e	1U, 2U, 8U	HP LTO6 HH FC	1.0.7.1, 02/11/2013 , podpisane	22EB
FlexStor II — 4U	2008 R2	5.2.3790.7, 06/06/2009 , podpisane	4.90/3.20 e	1U, 2U, 8U	HP LTO6 HH SAS	1.0.7.1, 02/11/2013 , podpisane	32CB
FlexStor II — 4U	2012	8.0.0.1, 07/05/2012 , podpisane	4.90/3.20 e	1U, 2U, 8U	HP LTO6 HH SAS	1.0.7.1, 02/11/2013 , podpisane	32CB
FlexStor II — 4U	2008 R2	5.2.3790.7, 06/06/2009 , podpisane	4.90/3.20 e	1U, 2U, 8U	IBM LTO6 HH FC	6.2.3.3, 10/29/2012 , podpisane	CBW5
FlexStor II — 4U	2012	8.0.0.1, 07/05/2012 , podpisane	4.90/3.20 e	1U, 2U, 8U	IBM LTO6 HH FC	6.2.3.3, 10/29/2012 , podpisane	CBW5
FlexStor II — 4U	2008 R2	5.2.3790.7, 06/06/2009 , podpisane	4.90/3.20 e	1U, 2U, 8U	IBM LTO6 HH SAS	6.2.3.3, 10/29/2012 , podpisane	CBW5

NAZWA MODELU BIBLIOTEKI	SYSTEM OPERACYJNY	WERSJA STEROWNIK A ZMIENIACZA	WERSJA OPROGRAM OWANIA UKŁADOWE GO BIBLIOTEKI	DODATKOW E BIBLIOTEKI W TEŚCIE	TYP STACJI TAŚM	WERSJA STEROWNIK A TAŚMY	WERSJA OPROGRAM OWANIA UKŁADOWE GO STACJI TAŚM
FlexStor II — 4U	2012	8.0.0.1, 07/05/2012 , podpisane	4.90/3.20 e	1U, 2U, 8U	IBM LTO6 HH SAS	6.2.3.3, 10/29/2012 , podpisane	CBW5
FlexStor II — 4U	2012\2012 R2	8.1.0.0, 01/07/2014 , podpisane	5.03/3.20 e	1U, 2U	IBM LTO7 HH FC	6.2.5.5, 09/08/2015 , podpisane	FA11
FlexStor II — 4U	2012\2012 R2	8.1.0.0, 01/07/2014 , podpisane	5.03/3.20 e	1U, 2U	IBM LTO7 HH SAS	6.2.5.5, 09/08/2015 , podpisane	FA11
FlexStor II — 4U	2012/2012 R2	8.1.0.0, 01/07/2014 , podpisane	5.40/3.20 e	1U, 2U	IBM LTO8 HH FC	6.2.6.6, 10/24/2017 , podpisane	HB81
FlexStor II — 4U	2012/2012 R2	8.1.0.0, 01/07/2014 , podpisane	5.40/3.20 e	1U, 2U	IBM LTO8 HH SAS	6.2.6.6, 10/24/2017 , podpisane	HB81
FlexStor II — 4U	2016	8.3.0.2. 07/03/2017 , podpisane	5.40/3.20 e	1U, 2U	IBM LT08 HH FC	6.2.6.6, 10/24/2017 , podpisane	HB81
FlexStor II — 4U	2016	8.3.0.2, 07/03/2017 , podpisane	5.40/3.20 e	1U, 2U	IBM LTO8 HH SAS	6.2.6.6, 10/24/2017 , podpisane	HB81
MultiStor	2012/2012 R2	8.1.0.0, 01/07/2014 , podpisane	1.1.0-0012		IBM LTO6 HH FC	6.2.6.6, 10/24/2017 , podpisane	H991
MultiStor	2012/2012 R2	8.1.0.0, 01/07/2014 , podpisane	1.1.0-0012		IBM LT06 HH SAS	6.2.6.6, 10/24/2017 , podpisane	H991
MultiStor	2012/2012 R2	8.1.0.0, 01/07/2014 , podpisane	1.1.0-0012		IBM LT07 HH FC	6.2.6.6, 10/24/2017 , podpisane	HB81
MultiStor	2012/2012 R2	8.1.0.0, 01/07/2014 , podpisane	1.1.0-0012		IBM LT07 HH SAS	6.2.6.6, 10/24/2017 , podpisane	HB81
MultiStor	2012/2012 R2	8.1.0.0, 01/07/2014 , podpisane	1.1.0-0012		IBM LT08 HH FC	6.2.6.6, 10/24/2017 , podpisane	HB81
MultiStor	2012/2012 R2	8.1.0.0, 01/07/2014 , podpisane	1.1.0-0012		IBM LT08 HH SAS	6.2.6.6, 10/24/2017 podpisany	HB81

NAZWA MODELU BIBLIOTEKI	SYSTEM OPERACYJNY	WERSJA STEROWNIK A ZMIENIACZA	WERSJA OPROGRAM OWANIA UKŁADOWE GO BIBLIOTEKI	DODATKOW E BIBLIOTEKI W TEŚCIE	TYP STACJI TAŚM	WERSJA STEROWNIK A TAŚMY	WERSJA OPROGRAM OWANIA UKŁADOWE GO STACJI TAŚM
MultiStor	2016	8.3.0.2, 07/03/2017 , podpisane	1.1.0-0012		IBM LT06 HH FC	6.2.6.6. 10/24/2017 , podpisane	H991
MultiStor	2016	8.3.0.2, 07/03/2017 , podpisane	1.1.0-0012		IBM LT06 HH SAS	6.2.6.6. 10/24/2017 , podpisane	H991
MultiStor	2016	8.3.0.2, 07/03/2017 , podpisane	1.1.0-0012		IBM LT07 HH FC	6.2.6.6. 10/24/2017 , podpisane	HB81
MultiStor	2016	8.3.0.2, 07/03/2017 , podpisane	1.1.0-0012		IBM LT07 HH SAS	6.2.6.6, 10/24/2017 , podpisane	HB81
MultiStor	2016	8.3.0.2, 07/03/2017 , podpisane	1.1.0-0012		IBM LT08 HH FC	6.2.6.6., 10/24/2017 , podpisane	HB81
MultiStor	2016	8.3.0.2, 07/03/2017 , podpisane	1.1.0-0012		IBM LT08 HH SAS	6.2.6.6, 10/24/2017 , podpisane	HB81
MULTISTAK	2012	8.3.0.0, 05/07/2014 , podpisane	1.7	-	HP LTO5 HH FC	1.0.7.1, 02/11/2013 , podpisane	Y64B
MULTISTAK	2012 R2	8.1.0.0, 01/07/2014 , podpisane	1.7	-	HP LTO5 HH FC	1.0.7.1, 02/11/2013 , podpisane	Y64B
MULTISTAK	2012	8.3.0.0, 05/07/2014 , podpisane	1.7	-	HP LTO5 HH SAS	1.0.7.1, 02/11/2013 , podpisane	Z64B
MULTISTAK	2012 R2	8.1.0.0, 01/07/2014 , podpisane	1.7	-	HP LTO5 HH SAS	1.0.7.1, 02/11/2013 , podpisane	Z64B
MULTISTAK	2012	8.3.0.0, 05/07/2014 , podpisane	1.7	-	HP LTO6 HH FC	1.0.7.1, 02/11/2013 , podpisane	238B
MULTISTAK	2012 R2	8.1.0.0, 01/07/2014 , podpisane	1.7	-	HP LTO6 HH FC	1.0.7.1, 02/11/2013 , podpisane	238B
MULTISTAK	2012	8.3.0.0, 05/07/2014 , podpisane	1.7	-	HP LTO6 HH SAS	1.0.7.1, 02/11/2013 , podpisane	338B

NAZWA MODELU BIBLIOTEKI	SYSTEM OPERACYJNY	WERSJA STEROWNIK A ZMIENIACZA	WERSJA OPROGRAM OWANIA UKŁADOWE GO BIBLIOTEKI	DODATKOW E BIBLIOTEKI W TEŚCIE	TYP STACJI TAŚM	WERSJA STEROWNIK A TAŚMY	WERSJA OPROGRAM OWANIA UKŁADOWE GO STACJI TAŚM
MULTISTAK	2012 R2	8.1.0.0, 01/07/2014 , podpisane	1.7	-	HP LTO6 HH SAS	1.0.7.1, 02/11/2013 , podpisane	338B
MULTISTAK	2012	8.3.0.0, 05/07/2014 , podpisane	1.7	-	IBM LTO5 HH FC	6.2.3.3, 10/29/2012 , podpisane	E4J6
MULTISTAK	2012 R2	8.1.0.0, 01/07/2014 , podpisane	1.7	-	IBM LTO5 HH FC	6.2.3.3, 10/29/2012 , podpisane	E4J6
MULTISTAK	2012	8.3.0.0, 05/07/2014 , podpisane	1.7	-	IBM LTO5 HH SAS	6.2.3.3, 10/29/2012 , podpisane	E4J6
MULTISTAK	2012 R2	8.1.0.0, 01/07/2014 , podpisane	1.7	-	IBM LTO5 HH SAS	6.2.3.3, 10/29/2012 , podpisane	E4J6
MULTISTAK	2012	8.3.0.0, 05/07/2014 , podpisane	1.7	-	IBM LTO6 HH FC	6.2.3.3, 10/29/2012 , podpisane	E4J6
MULTISTAK	2012 R2	8.1.0.0, 01/07/2014 , podpisane	1.7	-	IBM LTO6 HH FC	6.2.3.3, 10/29/2012 , podpisane	E4J6
MULTISTAK	2012	8.3.0.0, 05/07/2014 , podpisane	1.7	-	IBM LTO6 HH SAS	6.2.3.3, 10/29/2012 , podpisane	E4J6
MULTISTAK	2012 R2	8.1.0.0, 01/07/2014 , podpisane	1.7	-	IBM LTO6 HH SAS	6.2.3.3, 10/29/2012 , podpisane	E4J6
MULTISTAK	2012	8.3.0.0, 05/07/2014 , podpisane	1.7	-	HP LTO6 HH FC	1.0.7.1, 02/11/2013 , podpisane	238B
MULTISTAK	2012 R2	8.1.0.0, 01/07/2014 , podpisane	1.7	-	HP LTO6 HH FC	1.0.7.1, 02/11/2013 , podpisane	238B
MULTISTAK	2012	8.3.0.0, 05/07/2014 , podpisane	1.7	-	HP LTO6 HH SAS	1.0.7.1, 02/11/2013 , podpisane	338B
MULTISTAK	2012 R2	8.1.0.0, 01/07/2014 , podpisane	1.7	-	HP LTO6 HH SAS	1.0.7.1, 02/11/2013 , podpisane	338B

NAZWA MODELU BIBLIOTEKI	SYSTEM OPERACYJNY	WERSJA STEROWNIK A ZMIENIACZA	WERSJA OPROGRAM OWANIA UKŁADOWE GO BIBLIOTEKI	DODATKOW E BIBLIOTEKI W TEŚCIE	TYP STACJI TAŚM	WERSJA STEROWNIK A TAŚMY	WERSJA OPROGRAM OWANIA UKŁADOWE GO STACJI TAŚM
MULTISTAK	2012\2012 R2	8.3.0.0, 05/07/2014 , podpisane	2,05		IBM LTO7 HH FC	6.2.5.5, 09/08/2015 , podpisane	FA11
MULTISTAK	2012\2012 R2	8.3.0.0, 05/07/2014 , podpisane	2,05		IBM LTO7 HH SAS	6.2.5.5, 09/08/2015 , podpisane	FA11
MULTISTAK	2012\2012 R2	8.1.0.0, 01/07/2014 , podpisane	2.60		IBM LTO8 HH FC	6.2.6.6, 10/24/2017 , podpisane	HB81
MULTISTAK	2012\2012 R2	8.1.0.0, 01/07/2014 , podpisane	2.60		IBM LTO8 HH SAS	6.2.6.6, 10/24/2017 , podpisane	HB81
MULTISTAK	2016	8.3.0.2, 07/03/2017 , podpisane	2.60		IBM LTO8 HH FC	6.2.6.6, 10/24/2017 , podpisane	HB81
MULTISTAK	2016	8.3.0.2, 07/03/2017 , podpisane	2.60		IBM LTO8 HH SAS	6.2.6.6, 10/24/2017 , podpisane	HB81

Dell

NAZWA MODELU BIBLIOTEKI	SYSTEM OPERACYJNY	WERSJA STEROWNIKA ZMIENIACZA	WERSJA OPROGRAMO WANIA UKŁADOWEGO BIBLIOTEKI	TYP STACJI TAŚM	WERSJA STEROWNIKA TAŚMY	WERSJA OPROGRAMOW ANIA UKŁADOWEGO STACJI TAŚM
ML6000		Wersja v 2.6.2.1, A09	585G	LTO5 FH	6.1.9.9	B6W0
ML6000		Wersja v 2.6.2.1, A09	670G	LTO6 FH	6.3.9600.1638 4	F9A0
ML6000		Wersja v 2.6.2.1, A09	670G	LTO7 FH	6.3.9600.1638 4	FA10
TL1000		6.2.1.8	34	LTO5	6.2.1.8	B6W1
TL1000		6.2.3.3	58	LTO6	6.2.3.3	F9A1
TL1000		6.2.5.6	58	LTO7	6.2.5.6	FA11
TL1000		6.2.5.6	0106	LTO8	6.2.5.6	H9Ex
TL2000/4000		6.2.1.5	A. 50	LTO5 HH	6.2.1.5	B171

NAZWA MODELU BIBLIOTEKI	SYSTEM OPERACYJNY	WERSJA STEROWNIKA ZMIENIACZA	WERSJA OPROGRAMOWANIA UKŁADOWEGO BIBLIOTEKI	TYP STACJI TAŚM	WERSJA STEROWNIKA TAŚMY	WERSJA OPROGRAMOWANIA UKŁADOWEGO STACJI TAŚM
TL2000/4000		6.2.3.3	B, 60	LTO6 HH	6.2.3.3	C9T5
TL2000/4000		6.2.5.6	D. 10	LTO7 HH	6.2.5.6	FA11
ML3		6.2.6.5	1.1.1.0	LTO6	6.2.6.5	H99x
ML3		6.2.6.5	1.1.1.0	LTO7	6.2.6.5	H9Ex
ML3		6.2.6.5	1.1.1.0	LTO8	6.2.6.5	H9Ex

Fujitsu

NAZWA MODELU BIBLIOTEKI	SYSTEM OPERACYJNY	WERSJA STEROWNIKA ZMIENIACZA	WERSJA OPROGRAMOWANIA UKŁADOWEGO BIBLIOTEKI	DODATKOWE BIBLIOTEKI W TEŚCIE	TYP STACJI TAŚM	WERSJA STEROWNIKA TAŚMY	WERSJA OPROGRAMOWANIA UKŁADOWEGO STACJI TAŚM
ETERNUS LT60		7.7600.163 85.0, 01/02/2010 , podpisane	4.51/3,00 e	LT40	HP LTO5 FH FC	1.0.6.3, 10/07/2010 , podpisane	I24B
ETERNUS LT60		7.7600.163 85.0, 01/02/2010 , podpisane	4.51/3,00 e	LT40, LT20	HP LTO5 HH FC	1.0.6.3, 10/07/2010 , podpisane	Y23B
ETERNUS LT60		7.7600.163 85.0, 01/02/2010 , podpisane	4.51/3,00 e	LT40	SAS HP LTO5 FH	1.0.6.3, 10/07/2010 , podpisane	X22B
ETERNUS LT60		7.7600.163 85.0, 01/02/2010 , podpisane	4.51/3,00 e	LT40, LT20	HP LTO5 HH SAS	1.0.6.3, 10/07/2010 , podpisane	Z21B
ETERNUS LT60 S2	2008 R2	7.7600.163 85.1, 2/15/2011, podpisane	4.81/3.20 e	LT40 S2	HP LTO4 FH FC	1.0.7.1, 02/11/2013 , podpisane	H65B
ETERNUS LT60 S2	2012	8.0.0.1, 08/02/2012 , podpisane	4.81/3.20 e	LT40 S2	HP LTO4 FH FC	1.0.7.1, 02/11/2013 , podpisane	H65B
ETERNUS LT60 S2	2008 R2	7.7600.163 85.1, 2/15/2011, podpisane	4.81/3.20 e	LT40 S2	SAS HP LTO4 FH	1.0.7.1, 02/11/2013 , podpisane	A62B

NAZWA MODELU BIBLIOTEKI	SYSTEM OPERACYJNY	WERSJA STEROWNIK A ZMIENIACZA	WERSJA OPROGRAM OWANIA UKŁADOWE GO BIBLIOTEKI	DODATKOW E BIBLIOTEKI W TEŚCIE	TYP STACJI TAŚM	WERSJA STEROWNIK A TAŚMY	WERSJA OPROGRAM OWANIA UKŁADOWE GO STACJI TAŚM
ETERNUS LT60 S2	2012	8.0.0.1, 08/02/2012 , podpisane	4.81/3.20 e	LT40 S2	SAS HP LTO4 FH	1.0.7.1, 02/11/2013 , podpisane	A62B
ETERNUS LT60 S2	2008 R2	7.7600.163 85.1, 2/15/2011, podpisane	4.81/3.20 e	LT40 S2, LT20 S2	HP LTO4 HH FC	1.0.7.1, 02/11/2013 , podpisane	V63B
ETERNUS LT60 S2	2012	8.0.0.1, 08/02/2012 , podpisane	4.81/3.20 e	LT40 S2, LT20 S2	HP LTO4 HH FC	1.0.7.1, 02/11/2013 , podpisane	V63B
ETERNUS LT60 S2	2008 R2	7.7600.163 85.1, 2/15/2011, podpisane	4.81/3.20 e	LT40 S2, LT20 S2	HP LTO4 HH SAS	1.0.7.1, 02/11/2013 , podpisane	U64B
ETERNUS LT60 S2	2012	8.0.0.1, 08/02/2012 , podpisane	4.81/3.20 e	LT40 S2, LT20 S2	HP LTO4 HH SAS	1.0.7.1, 02/11/2013 , podpisane	U64B
ETERNUS LT60 S2		7.7600.163 85.1, 02/15/2011 , podpisane	4.60/3.10 e	LT40 S2	HP LTO5 FH FC	1.0.6.3, 10/07/2010 , podpisane	I24B
ETERNUS LT60 S2		7.7600.163 85.1, 02/15/2011 , podpisane	4.60/3.10 e	LT40 S2, LT20 S2	HP LTO5 HH FC	1.0.6.3, 10/07/2010 , podpisane	Y34B
ETERNUS LT60 S2		7.7600.163 85.1, 02/15/2011 , podpisane	4.60/3.10 e	LT40 S2	SAS HP LTO5 FH	1.0.6.3, 10/07/2010 , podpisane	X22B
ETERNUS LT60 S2		7.7600.163 85.1, 02/15/2011 , podpisane	4.60/3.10 e	LT40 S2, LT20 S2	HP LTO5 HH SAS	1.0.6.3, 10/07/2010 , podpisane	Z21B
ETERNUS LT60 S2	2008 R2	7.7600.163 85.1, 2/15/2011, podpisane	4.81/3.20 e	LT40 S2, LT20 S2	HP LTO6 HH FC	1.0.7.1, 02/11/2013 , podpisane	22EB
ETERNUS LT60 S2	2012	8.0.0.1, 08/02/2012 , podpisane	4.81/3.20 e	LT40 S2, LT20 S2	HP LTO6 HH FC	1.0.7.1, 02/11/2013 , podpisane	22EB

NAZWA MODELU BIBLIOTEKI	SYSTEM OPERACYJNY	WERSJA STEROWNIK A ZMIENIACZA	WERSJA OPROGRAM OWANIA UKŁADOWE GO BIBLIOTEKI	DODATKOW E BIBLIOTEKI W TEŚCIE	TYP STACJI TAŚM	WERSJA STEROWNIK A TAŚMY	WERSJA OPROGRAM OWANIA UKŁADOWE GO STACJI TAŚM
ETERNUS LT60 S2	2008 R2	7.7600.163 85.1, 2/15/2011, podpisane	4.81/3.20 e	LT40 S2, LT20 S2	HP LTO6 HH SAS	1.0.7.1, 02/11/2013 , podpisane	32CB
ETERNUS LT60 S2	2012	8.0.0.1, 08/02/2012 , podpisane	4.81/3.20 e	LT40 S2, LT20 S2	HP LTO6 HH SAS	1.0.7.1, 02/11/2013 , podpisane	32CB
ETERNUS LT60 S2	2012\2012 R2	8.2.0.1, 05/22/2014 , podpisane	4.88/3.20 e	ETERNUS LT20 S2 ETERNUS LT40 S2	IBM LTO6 HH FC	6.2.5.5, 09/08/2015 , podpisane	F9A1
ETERNUS LT60 S2	2012\2012 R2	8.2.0.1, 05/22/2014 , podpisane	4.88/3.20 e	ETERNUS LT20 S2 ETERNUS LT40 S2	IBM LTO6 HH SAS	6.2.5.5, 09/08/2015 , podpisane	F9A1
ETERNUS LT60 S2	2012\2012 R2	8.2.0.1, 05/22/2014 , podpisane	4.88/3.20 e	ETERNUS LT20 S2 ETERNUS LT40 S2	IBM LTO7 HH FC	6.2.5.5, 09/08/2015 , podpisane	FA11
ETERNUS LT60 S2	2012\2012 R2	8.2.0.1, 05/22/2014 , podpisane	4.88/3.20 e	ETERNUS LT20 S2 ETERNUS LT40 S2	IBM LTO7 HH SAS	6.2.5.5, 09/08/2015 , podpisane	FA11
ETERNUS LT60 S2	2012/2012 R2	8.2.0.1, 05/22/2014 , podpisane	5.10/3.20 e	ETERNUS LT20 S2 ETERNUS LT40 S2	IBM LTO8 HH FC	6.2.6.6, 10/24/2017 , podpisane	HB81
ETERNUS LT60 S2	2012\2012 R2	8.2.0.1, 05/22/2014 , podpisane	5.10/3.20 e	ETERNUS LT20 S2 ETERNUS LT40 S2	IBM LTO8 HH SAS	6.2.6.6, 10/24/2017 , podpisane	HB81
ETERNUS LT60 S2	2016	8.2.0.6, 07/03/2017 , podpisane	5.10/3.20 e	ETERNUS LT20 S2 ETERNUS LT40 S2	IBM LTO8 HH FC	6.2.6.6, 10/24/2017 , podpisane	HB81
ETERNUS LT60 S2	2016	8.2.0.6, 07/03/2017 , podpisane	5.10/3.20 e	ETERNUS LT20 S2 ETERNUS LT40 S2	IBM LTO8 HH SAS	6.2.6.6, 10/24/2017 , podpisane	HB81
ETERNUS LT140	2012R2	8.2.0.1, 05/22/2014 , podpisane	1.0.0 — A00		IBM LTO6 HH FC LTO6 HH SAS	6.2.6.6, 10/24/2017 , podpisane	JAX1

NAZWA MODELU BIBLIOTEKI	SYSTEM OPERACYJNY	WERSJA STEROWNIK A ZMIENIACZA	WERSJA OPROGRAM OWANIA UKŁADOWE GO BIBLIOTEKI	DODATKOW E BIBLIOTEKI W TEŚCIE	TYP STACJI TAŚM	WERSJA STEROWNIK A TAŚMY	WERSJA OPROGRAM OWANIA UKŁADOWE GO STACJI TAŚM
ETERNUS LT140	2012R2	8.2.0.1, 05/22/2014 , podpisane	1.0.0 — A00		IBM LTO7 HH FC LTO7 HH SAS	6.2.6.6, 10/24/2017 , podpisane	JAY1
ETERNUS LT140	2012R2	8.2.0.1, 05/22/2014 , podpisane	1.0.0 — A00		IBM LTO8 HH FC LTO8 HH SAS	6.2.6.6, 10/24/2017 , podpisane	JAY1
ETERNUS LT140	2016	8.2.0.6, 07/03/2017 , podpisane	1.0.0 — A00		IBM LTO6 HH FC LTO6 HH SAS	6.2.6.6, 10/24/2017 , podpisane	JAX1
ETERNUS LT140	2016	8.2.0.6, 07/03/2017 , podpisane	1.0.0 — A00		IBM LTO7 HH FC LTO7 HH SAS	6.2.6.6, 10/24/2017 , podpisane	JAY1
ETERNUS LT140	2016	8.2.0.6, 07/03/2017 , podpisane	1.0.0 — A00		IBM LTO8 HH FC IBM LTO HH SAS	6.2.6.6, 10/24/2017 , podpisane	JAY1
ETERNUS LT260	2012	8.2.0.1, 05/22/2014 , podpisane	6.1		HP LTO4 FH FC	1.0.7.1, 02/11/2013 , podpisane	H66B
ETERNUS LT260	2012 R2	8.2.0.1, 05/22/2014 , podpisane	6.1		HP LTO4 FH FC	1.0.7.1, 02/11/2013 , podpisane	H66B
ETERNUS LT260		8.2.0.1, 05/22/2014 , podpisane	6.1		HP LTO4 FH FC	1.0.7.1, 02/11/2013 , podpisane	V64B
ETERNUS LT260	2012	8.2.0.1, 05/22/2014 , podpisane	6.1		HP LTO5FH FC	1.0.7.1, 02/11/2013 , podpisane	I66B
ETERNUS LT260	2012 R2	8.2.0.1, 05/22/2014 , podpisane	6.1		HP LTO5 FH FC	1.0.7.1, 02/11/2013 , podpisane	I66B
ETERNUS LT260	2012	8.2.0.1, 05/22/2014 , podpisane	6.1		HP LTO5 HH FC	1.0.7.1, 02/11/2013 , podpisane	Y67B
ETERNUS LT260	2012 R2	8.2.0.1, 05/22/2014 , podpisane	6.1		HP LTO5 HH FC	1.0.7.1, 02/11/2013 , podpisane	Y67B

NAZWA MODELU BIBLIOTEKI	SYSTEM OPERACYJNY	WERSJA STEROWNIK A ZMIENIACZA	WERSJA OPROGRAM OWANIA UKŁADOWE GO BIBLIOTEKI	DODATKOW E BIBLIOTEKI W TEŚCIE	TYP STACJI TAŚM	WERSJA STEROWNIK A TAŚMY	WERSJA OPROGRAM OWANIA UKŁADOWE GO STACJI TAŚM
ETERNUS LT260	2012	8.2.0.1, 05/22/2014 , podpisane	6.1		HP LTO5 HH SAS	1.0.7.1, 02/11/2013 , podpisane	Z67B
ETERNUS LT260	2012 R2	8.2.0.1, 05/22/2014 , podpisane	6.1		HP LTO5 HH SAS	1.0.7.1, 02/11/2013 , podpisane	Z67B
ETERNUS LT260	2012	8.2.0.1, 05/22/2014 , podpisane	6.1		HP LTO6 HH FC	1.0.7.1, 02/11/2013 , podpisane	238B
ETERNUS LT260	2012 R2	8.2.0.1, 05/22/2014 , podpisane	6.1		HP LTO6 HH FC	1.0.7.1, 02/11/2013 , podpisane	238B
ETERNUS LT260	2012	8.2.0.1, 05/22/2014 , podpisane	6.1		HP LTO6 HH SAS	1.0.7.1, 02/11/2013 , podpisane	338B
ETERNUS LT260	2012R2	8.2.0.1, 05/22/2014 , podpisane	6.1		HP LTO6 HH SAS	1.0.7.1, 02/11/2013 , podpisane	338B
ETERNUS LT260	2012\2012 R2	8.2.0.1, 05/22/2014 , podpisane	6,71		IBMLTO6 HH FC	6.2.5.5, 09/08/2015 , podpisane	FA91
ETERNUS LT260	2012\2012 R2	8.2.0.1, 05/22/2014 , podpisane	6,71		IBMLTO6 HH SAS	6.2.5.5, 09/08/2015 , podpisane	FA91
ETERNUS LT260	2012\2012 R2	8.2.0.1, 05/22/2014 , podpisane	6,71		IBMLTO7 HH FC	6.2.5.5, 09/08/2015 , podpisane	FA11
ETERNUS LT260	2012\2012 R2	8.2.0.1, 05/22/2014 , podpisane	6,71		IBM LTO7 HH SAS	6.2.5.5, 09/08/2015 , podpisane	FA11
ETERNUS LT260	2012\2012 R2	8.2.0.1, 05/22/2014 , podpisane	7,50		IBM LTO8 HH FC	6.2.6.6, 10/24/2017 , podpisane	HB81
ETERNUS LT260	2012\2012 R2	8.2.0.1, 05/22/2014 , podpisane	7,50		IBM LTO8 HH SAS	6.2.6.6, 10/24/2017 , podpisane	HB81
ETERNUS LT260	2016	8.2.0.6, 07/03/2017 , podpisane	7,50		IBM LTO8 HH FC	6.2.6.6, 10/24/2017 , podpisane	HB81

NAZWA MODELU BIBLIOTEKI	SYSTEM OPERACYJNY	WERSJA STEROWNIK A ZMIENIACZA	WERSJA OPROGRAM OWANIA UKŁADOWE GO BIBLIOTEKI	DODATKOW E BIBLIOTEKI W TEŚCIE	TYP STACJI TAŚM	WERSJA STEROWNIK A TAŚMY	WERSJA OPROGRAM OWANIA UKŁADOWE GO STACJI TAŚM
ETERNUS LT260	2016	8.2.0.6, 07/03/2017 , podpisane	7,50		IBM LTO8 HH SAS	6.2.6.6, 10/24/2017 , podpisane	HB81

Hewlett Packard Enterprise

NAZWA MODELU BIBLIOTEKI	SYSTEM OPERACYJNY	WERSJA STEROWNIKA ZMIENIACZA	WERSJA OPROGRAMO WANIA UKŁADOWEGO BIBLIOTEKI	TYP STACJI TAŚM	WERSJA STEROWNIKA TAŚMY	WERSJA OPROGRAMOW ANIA UKŁADOWEGO STACJI TAŚM
Stacja autonomiczna		Brak	Brak	HPE LTO7 HPE LTO8	1.0.9.1 lub nowsza 1.0.9.3 lub nowsza	G9Q1 lub nowszy J4DB lub nowszy
StoreOnce VTL		Sterowniki taśm HP StoreEver dla systemu Windows v 4.0.0.0 lub nowsze	3.11. x lub nowszy	Dyski z HP LTO	Sterowniki taśm HP StoreEver dla systemu Windows v 4.0.0.0 lub nowsze	Brak
ESL G3		Sterowniki taśm HP StoreEver dla systemu Windows v 4.0.0.0 lub nowsze	680H. GS50501 MCB2 lub nowszy 656H. GS10801 MCB1 lub nowszy	HPE LTO7 FH FC HP LTO6 FH FC HP LTO5 FH FC HP LTO4 FH FC	Sterowniki taśm HP StoreEver dla systemu Windows v 4.0.0.0 lub nowsze	FA18 lub nowszy J3PW lub nowszy I6GW lub nowszy H6HW lub nowszy

NAZWA MODELU BIBLIOTEKI	SYSTEM OPERACYJNY	WERSJA STEROWNIKA ZMIENIACZA	WERSJA OPROGRAMO WANIA UKŁADOWEGO BIBLIOTEKI	TYP STACJI TAŚM	WERSJA STEROWNIKA TAŚMY	WERSJA OPROGRAMOW ANIA UKŁADOWEGO STACJI TAŚM
MSL 6480		Sterowniki taśm HP StoreEver dla systemu Windows v 4.4.0.0 lub nowszego	4,60 lub nowszy	HPE LTO8 HH FC	Sterowniki taśm HPE StoreEver dla systemu Windows v 4.4.0.0 lub nowszego	J4DB lub nowszy
				HPE LTO8 HH SAS		J4DB lub nowszy
				HPE LTO7 HH FC		FA17 lub nowszy
				HPE LTO7 HH SAS		FA17 lub nowszy
				HP LTO6 HH FCHP LTO6 HH SAS		252W lub nowszy
				HP LTO5 FH FC		352W lub nowszy
				HP LTO5 HH FC		I6GW lub nowszy
				HP LTO5 HH SAS		Y6DW lub nowszy
				HP LTO4 FH FC		Z6DW lub nowszy
				HP LTO4 HH SAS		H6FW lub nowszy
MSL 3040		Sterowniki taśm HP StoreEver dla systemu Windows v 4.4.0.0 lub nowszego	3210 lub nowszy	HPE LTO8 HH FC	Sterowniki taśm HP StoreEver dla systemu Windows v 4.4.0.0 lub nowszego	J4DB lub nowszy
				HPE LTO8 HH SAS		J4DB lub nowszy

NAZWA MODELU BIBLIOTEKI	SYSTEM OPERACYJNY	WERSJA STEROWNIKA ZMIENIACZA	WERSJA OPROGRAMOWANIA UKŁADOWEGO BIBLIOTEKI	TYP STACJI TAŚM	WERSJA STEROWNIKA TAŚMY	WERSJA OPROGRAMOWANIA UKŁADOWEGO STACJI TAŚM
Rodzina MSL G3		Sterowniki taśm HP StoreEver dla systemu Windows v 4.4.0.0 lub nowszego	MSL8096- 1130 lub nowszy	HPE LTO8 HH FC	Sterowniki taśm HPE StoreEver dla systemu Windows v 4.4.0.0 lub nowszego	J4DB lub nowszy
			MSL4048- 8.70 lub nowszy	HPE LTO8 HH SAS		J4DB lub nowszy
			MSL2024- 6.20 lub nowszy	HPE LTO7 HH FC		FA17 lub nowszy
				HPE LTO7 HH SAS		FA17 lub nowszy
				HP LTO6 HH FC		252W lub nowszy
				HP LTO6 HH SAS		352W lub nowszy
				HP LTO5 FH FC		I6GW lub nowszy
				HP LTO5 HH FC		Y6DW lub nowszy
				HP LTO5 HH SAS		Z6DW lub nowszy
				HP LTO4 FH FC		H6FW lub nowszy
				HP LTO4 HH SAS		U62W lub nowszy

NAZWA MODELU BIBLIOTEKI	SYSTEM OPERACYJNY	WERSJA STEROWNIKA ZMIENIACZA	WERSJA OPROGRAMO WANIA UKŁADOWEGO BIBLIOTEKI	TYP STACJI TAŚM	WERSJA STEROWNIKA TAŚMY	WERSJA OPROGRAMOW ANIA UKŁADOWEGO STACJI TAŚM
Automatyczna ładowarka G2 1/8		Sterowniki taśm HP StoreEver dla systemu Windows v 4.4.0.0 lub nowsze	4,30 lub nowszy	HPE LTO8 HH FC	Sterowniki taśm HPE StoreEver dla systemu Windows v 4.4.0.0 lub nowsze	J4DB lub nowszy
				HPE LTO8 HH SAS		J4DB lub nowszy
				HPE LTO7 HH FC		FA17 lub nowszy
				HPE LTO7 HH SAS		FA17 lub nowszy
				HP LTO6 HH FC		252W lub nowszy
				HP LTO6 HH SAS		352W lub nowszy
				HP LTO5 HH FC		Y6DW lub nowszy
				HP LTO5 HH SAS		Z6DW lub nowszy
				HP LTO4 HH SAS		U62W lub nowszy

IBM

NAZWA MODELU BIBLIOTEKI	SYSTEM OPERACYJNY	WERSJA STEROWNIKA ZMIENIACZA	WERSJA OPROGRAMO WANIA UKŁADOWEGO BIBLIOTEKI	TYP STACJI TAŚM	WERSJA STEROWNIKA TAŚMY	WERSJA OPROGRAMOW ANIA UKŁADOWEGO STACJI TAŚM
Stacja autonomiczna		Brak	Brak	Autonomiczna IBM LTO5 FH	Skrzynka odbiorcza programu Ltotape. sys	
Łączny magazyn 3572 (TS2900)		ibmcp2k12, 6.2.3.3	B. 50	LTO6 HH SAS	ibmcp2k12, 6.2.3.3	CB21
Łączny magazyn 3572 (TS2900)		ibmcp2k8, 6.2.1.8, x64	17	LTO5 HH SAS	ibmtp2k8, 6.2.1.8, x64	B6W1
Łączny magazyn 3573		ibmcp2k8, 6.2.1.8, x64	A. 40	IBM LTO5 3580	ibmtp2k8, 6.2.1.8, x64	B6W0

NAZWA MODELU BIBLIOTEKI	SYSTEM OPERACYJNY	WERSJA STEROWNIKA ZMIENIACZA	WERSJA OPROGRAMO WANIA UKŁADOWEGO BIBLIOTEKI	TYP STACJI TAŚM	WERSJA STEROWNIKA TAŚMY	WERSJA OPROGRAMOW ANIA UKŁADOWEGO STACJI TAŚM
Łączny magazyn 3573 (TS3100/TS3200)		ibmcg2k12, 6.2.3.3	B. 50	LTO6 FH FC	ibmcg2k12, 6.2.3.3	C9T4
Łączny magazyn 3573 (TS3100/TS3200)		ibmcg2k8, 6.2.1.8, x64	A. 40	LTO4 FH FC	ibmcg2k8, 6.2.1.8, x64	A230
Łączny magazyn 3573 (TS3100/TS3200)		ibmcg2k12, 6.2.3.3	B. 50	LTO6 HH SAS	ibmcg2k12, 6.2.3.3	C9T5
Łączny magazyn 3576 (TS3310)		ibmcg2k12, 6.2.3.3	630G	LTO6 FH FC	ibmcg2k12, 6.2.3.3	CB20
Łączny magazyn 3584 (TS3500/TS4500)	2012/2012R2	6.2.5.6	F030	LTO6 FH FC	6.2.5.6	F9A0
Łączny magazyn 3572 (TS2900)	2012/2012R2	6.2.5.6	58	LTO7 HH SAS	6.2.5.6	FA11
Łączny magazyn 3573 (TS3100)	2012/2012R2	6.2.5.6	D. 00	LTO7 FH FC	6.2.5.6	FA10
Łączny magazyn 3573 (TS3100)	2012/2012R2	6.2.5.6	D. 00	LTO7 HH FC/SAS	6.2.5.6	FA11
Łączny magazyn 3573 (TS3200)	2012/2012R2	6.2.5.6	D. 00	LTO7 FH FC	6.2.5.6	FA10
Łączny magazyn 3573 (TS3200)	2012/2012R2	6.2.5.6	D. 00	LTO7 HH FC/SAS	6.2.5.6	FA11

NAZWA MODELU BIBLIOTEKI	SYSTEM OPERACYJNY	WERSJA STEROWNIKA ZMIENIACZA	WERSJA OPROGRAMO WANIA UKŁADOWEGO BIBLIOTEKI	TYP STACJI TAŚM	WERSJA STEROWNIKA TAŚMY	WERSJA OPROGRAMOW ANIA UKŁADOWEGO STACJI TAŚM
Łączny magazyn 3576 (TS3310)	2012/2012R2	6.2.5.6	670G	LTO7 FH FC	6.2.5.6	FA10
Łączny magazyn 3584 (TS3500/TS45 00)	2012/2012R2	6.2.5.6	F030/1201	LTO7 FH FC	6.2.5.6	F980
Łączny magazyn 3584 (TS4500/TS35 00)		6.2.6.6	1413/G060	LTO8	6.2.6.6	J4D0
Łączny magazyn 3573 (TS4300/TS32 00/TS3100)		6.2.6.6	1112/F00	LTO8	6.2.6.6	J4D0/J4D1
Łączny magazyn 3572 (TS2900)		6.2.6.6	0080	LTO8	6.2.6.6	HB83

TIP

Należy dodać następujący klucz rejestru, aby włączyć obsługę TS 2900: DWORD "RSMCompatMode" w obszarze "HKEY_LOCAL_MACHINE \SOFTWARE\Microsoft\Microsoft Data Protection Manager " i ustawić ją na 29 (dziesiętny).

Kwantowe

NAZWA MODELU BIBLIOTEKI	SYSTEM OPERACYJNY	WERSJA STEROWNIK A ZMIENIACZA	WERSJA OPROGRAM OWANIA UKŁADOWE GO BIBLIOTEKI	DODATKOW E BIBLIOTEKI W TEŚCIE	TYP STACJI TAŚM	WERSJA STEROWNIK A TAŚMY	WERSJA OPROGRAM OWANIA UKŁADOWE GO STACJI TAŚM
DXi6701 skalarny (emulowani e i2000)		Qi2Kx64.sys , 7.5.0.0	V 2.1.1	DXi6702	HP LTO5	hplto.sys, 1.6.0.3	I30Z
DXi6701 skalarny (emulowani e i2000)		Qi2Kx64.sys , 7.5.0.0	V 2.1.1	DXi6702	LTO5 IBM	ibmtp2k8. sys, 6.2.1.8	A5MO

NAZWA MODELU BIBLIOTEKI	SYSTEM OPERACYJNY	WERSJA STEROWNIK A ZMIENIACZA	WERSJA OPROGRAM OWANIA UKŁADOWE GO BIBLIOTEKI	DODATKOW E BIBLIOTEKI W TEŚCIE	TYP STACJI TAŚM	WERSJA STEROWNIK A TAŚMY	WERSJA OPROGRAM OWANIA UKŁADOWE GO STACJI TAŚM
DXi8500 2 TB (emulowani e i2000)		Qi2Kx64.sys , 7.5.0.0	V1.5.0_85		HP LTO4	hplto.sys, 1.6.0.3	H44Z
DXi8500 2 TB (emulowani e i2000)		Qi2Kx64.sys , 7.5.0.0	V1.5.0_85		IBM LTO4	ibmtp2k8. sys, 6.2.1.8	A2FB
DXi8502 (VTL)		Qi500X64.s ys, 7.5.0.0	2.0.2_85		HP LTO5	hplto.sys, 1.6.0.3	I30Z
DXi6902 (VTL)		Qi2kx64.sys , 7.6.1.0	3.0		HP LTO5IBM LTO5	hplto.yyx,1. 0.7.16.2.92 00.16348	I6PZF990
DXi6902 (VTL) emulacja skalarnej i6000	Windows 2016	QntmLib.sy s 1.0.0.1	3.2.5		LTO5 IBM	ibmtp2k16 6.2.6.1	A5M0
DXi4701 (VTL)		Qi2kx64.sys , 7.6.1.0	3.0		HP LTO5IBM LTO5	hplto.yyx,1. 0.7.16.2.92 00.16348	I6PZF990
DXi4701 (VTL) emulacja skalarnej i6000	Windows 2016	QntmLib.sy s 1.0.0.1	3.2.5		LTO5 IBM	ibmtp2k16 6.2.6.1	A5M0
Skalarny i40		Qi40X64.sy s, 7.5.2.0	130G		HP LTO5	hplto.sys, 1.6.0.2	Y35Z
Skalarny i40		Qi40X64.sy s, 7.6.0.0	175G		LTO6 IBM	6.3.9600.16 384	F3JD
Skalarny i40		Qi40X64.sy s, 7.6.0.0	180B		IBM LTO7	6.3.9600.16 384	FA17
Skalarny i80		Qi40X64.sy s, 7.5.2.0	130G		HP LTO5	hplto.sys, 1.6.0.2	Y35Z
Skalarny i80		Qi40X64.sy s, 7.6.0.0	175G		LTO6 IBM	6.3.9600.16 384	F3JD
Skalarny i80		Qi40X64.sy s, 7.6.0.0	180G		IBM LTO7	6.3.9600.16 384	FA17

NAZWA MODELU BIBLIOTEKI	SYSTEM OPERACYJNY	WERSJA STEROWNIK A ZMIENIACZA	WERSJA OPROGRAM OWANIA UKŁADOWE GO BIBLIOTEKI	DODATKOW E BIBLIOTEKI W TEŚCIE	TYP STACJI TAŚM	WERSJA STEROWNIK A TAŚMY	WERSJA OPROGRAM OWANIA UKŁADOWE GO STACJI TAŚM
Skalarny i500		ad500x64.s ys, 7.4.0.0	500G		IBM LTO4	ibmtp2k3. sys, 6.1.8.9	82FB
Skalarny i500		Qi500X64.s ys, 7.5.0.0	607G		HP LTO5	hplto.sys, 1.6.0.2	I3EZ
Skalarny i500		Qi500X64.s ys, 7.5.0.0	607G		LTO5 IBM	ibmtp2k8. sys, 6.1.9.9	B170
Skalarny i500		Qi500X64.s ys, 7.5.0.0	607G		HP LTO4	hplto.sys, 1.6.0.2	H58Z
Skalarny i500		Qi500x64.s ys, 7.6.0.0	670G		LTO6 IBM	6.3.9600.16 384	F9A0
Skalarny i500		Qi500x64.s ys, 7.6.0.0	670G		IBM LTO7	6.3.9600.16 384	FA10
Skalarny i500	Windows 2016	QtmLib 1.0.0.1	700G		LTO8 IBM	programu Ltotape 10.0.14393. 206	H7TF
Skalarny i6000		Qi6Kx64.sys , 7.5.5.0	606A.GS00 301	Skalarny i2000	HP LTO4 FC	hplto.sys, 1.6.0.1	H58Z
Skalarny i6000		Qi6Kx64.sys , 7.5.5.0	606A.GS00 301	Skalarny i2000	HP LTO5 FC	hplto.sys, 1.6.0.1	I3AZ
Skalarny i6000		Qi6Kx64.sys , 7.5.5.0	606A.GS00 301	Skalarny i2000	IBM LTO5 FC	lto.sys, 6.1.7600.16 385	A6SA
Skalarny i6000		Qi6Kx64.sys , 7.5.5.0	606A.GS00 301	Skalarny i2000	IBM LTO5 FC	lto.sys, 6.1.7600.16 385	B170
Skalarny i6000		Qi6Kx64.sys , 7.5.5.0	606A.GS00 301	Skalarny i2000	IBM LTO4 FC	lto.sys, 6.1.7600.16 385	A23D
Skalarny i6000		Qi6kx64.sys , 7.6.1.0	720Q		LTO6 IBM	6.3.9600.16 384	F9A0
Skalarny i6000		Qi6kx64.sys , 7.6.1.0	720Q		IBM LTO7	6.3.9600.16 384	FA10
Skalarny i6000	Windows 2016	QntmLib 1.0.0.1	760Q		LTO8 IBM	programu Ltotape 10.0.14393. 206	H980

NAZWA MODELU BIBLIOTEKI	SYSTEM OPERACYJNY	WERSJA STEROWNIK A ZMIENIACZA	WERSJA OPROGRAM OWANIA UKŁADOWE GO BIBLIOTEKI	DODATKOW E BIBLIOTEKI W TEŚCIE	TYP STACJI TAŚM	WERSJA STEROWNIK A TAŚMY	WERSJA OPROGRAM OWANIA UKŁADOWE GO STACJI TAŚM
Przeciążenie		QsmcX64.syr, 2.5.1.0	V61		LTO4 Quantum	QLTOx64.syr, 3.4.0	2103
Przeciążenie		QsmcX64.syr, 2.6.2.0	75		LTO5 Quantum	QLTOx64.syr, 3.4.0.0	3060
Przeciążenie		QsmcX64.syr, 2.6.3.0	V91		LTO5 IBM	6.3.9600.16 384	F3HB
Przeciążenie		QsmcX64.syr, 2.6.3.0	V91		LTO6 IBM	6.3.9600.16 384	F3JD
Przeciążenie		QsmcX64.syr, 2.6.3.0	V92		IBM LTO7	6.3.9600.16 384	FA17
Przeciążenie	Windows 2016	QntmLib, 1.0.0.1	V94		LTO8 IBM	programu Ltotope 10.0.14393. 206	H7TF
Skalarny i3		6.3.9600.16 384	110G		IBM LTO6 HH	6.3.9600.16 384	G9P1
Skalarny i3		6.3.9600.16 384	110G		IBM LTO7 HH	6.3.9600.16 384	G9Q1
Skalarny i3	Windows 2016	QntmLib 1.0.0.1	150G		IBM LTO8 HH	programu Ltotope 10.0.14393. 206	H7TF
Skalarny i6		6.3.9600.16 384	110G		LTO6 IBM	6.3.9600.16 384	G9P0
Skalarny i6		6.3.9600.16 384	110G		IBM LTO7	6.3.9600.16 384	G9Q0
Skalarny i6	Windows 2016	QntmLib 1.0.0.1	150G		LTO8 IBM	programu Ltotope 10.0.14393. 206	H7TF

Dane firmy Tandberg

NAZWA MODELU BIBLIOTEKI	SYSTEM OPERACYJNY	WERSJA STEROWNIK A ZMIENIACZA	WERSJA OPROGRAM OWANIA UKŁADOWE GO BIBLIOTEKI	DODATKOW E BIBLIOTEKI W TEŚCIE	TYP STACJI TAŚM	WERSJA STEROWNIK A TAŚMY	WERSJA OPROGRAM OWANIA UKŁADOWE GO STACJI TAŚM
StorageLoa der LTO		1.8.0.11	3.47		HP 3000 LTO 5 HH SAS	1.0.6.1	Z21U
StorageLoa der LTO		1.8.0.11	3.47		HP 3000 LTO 5 HH SAS	1.0.6.1	Z33U
		exbchg64. sys, 2.1.9.0, 11/21/2008 , podpisane, 64-bitowe	V1C270		LTO4	hplto. sys, 1.0.5.2, 12/10/2007 , podpisane, 64-bitowe	D217
		exachgx64. sys, 2.1.9.0, 11/21/2008 , unsigned, 64-bitowy	V1C270		LTO4	ibmtp2k8. sys, 6.1.8.9, 3/19/2008, podpisane, 64-bitowe	85V3
		exbchg64. sys, 2.1.9.0, 11/21/2008 , podpisane, 64-bitowe	V1D170		LTO4	ibmtp2k8. sys, 6.1.9.5, 6/11/2008, podpisane, 64-bitowe	85V3
		exachgx64. sys, 2.1.9.0, 11/21/2008 , unsigned, 64-bitowy	V1D170		LTO4	ibmtp2k3. sys, 6.1.8.9, 3/19/2008, podpisane, 64-bitowe	85V3
		3.01.0009.0	V1C290	Magnum 224, StorageLoa der 2U	HP 3000 LTO 5 HH SAS	1.0.6.1	Z21U
		3.01.0009.0	V1C290	Magnum 224, StorageLoa der 2U	HP 3000 LTO 5 HH SAS	1.0.6.1	Z33U
		3.01.0009.0	V1C290	Magnum 224, StorageLoa der 2U	HP 3000 LTO 5 HH FC	1.0.6.1	Y21U
		3.01.0009.0	V1C290	Magnum 224, StorageLoa der 2U	HP 3000 LTO 5 HH FC	1.0.6.1	Y31U

NAZWA MODELU BIBLIOTEKI	SYSTEM OPERACYJNY	WERSJA STEROWNIK A ZMIENIACZA	WERSJA OPROGRAM OWANIA UKŁADOWE GO BIBLIOTEKI	DODATKOW E BIBLIOTEKI W TEŚCIE	TYP STACJI TAŚM	WERSJA STEROWNIK A TAŚMY	WERSJA OPROGRAM OWANIA UKŁADOWE GO STACJI TAŚM
		3.01.0009.0	V1C290	Magnum 224, StorageLoa der 2U	HP 3000 LTO 5 HH FC	1.0.6.1	Y32U
		3.01.0009.0	V1C290	Magnum 224, StorageLoa der 2U	HP 1760 LTO 4 HH FC	1.0.6.1	V51U
		3.01.0009.0	V1C290	Magnum 224, StorageLoa der 2U	HP 1760 LTO 4 HH SAS	1.0.6.1	U51U
		3.01.0009.0	V1C290	Magnum 224, StorageLoa der 2U	HP 1760 LTO 4 HH SCSI	1.0.6.1	W51U
		tdsafe. sys, 1.7.0.0, 1/4/2008, podpisane, 64-bitowe	3.42		LTO4	hplto. sys, 1.0.5.2, 12/10/2007 , podpisane, 64-bitowe	W22U
		tdsafe. sys, 1.7.0.0, 1/4/2008, podpisane, 64-bitowe	3.8		LTO4	programu Ltotape. sys, 6.0.6001.18 000, 6/21/2006, podpisane, 64-bitowe	85V3
		tdsafe. sys, 1.7.0.0, 1/4/2008, podpisane, 64-bitowe	3,63		LTO4	ibmtp2k8. sys, 6.1.8.9, 3/19/2008, podpisane, 64-bitowe	85V3
		1.8.0.11	3.47		HP 3000 LTO 5 HH FC	1.0.6.1	Y21U
		1.8.0.11	3.47		HP 3000 LTO 5 HH FC	1.0.6.1	Y31U
		1.8.0.11	3.47		HP 3000 LTO 5 HH FC	1.0.6.1	Y32U

NAZWA MODELU BIBLIOTEKI	SYSTEM OPERACYJNY	WERSJA STEROWNIK A ZMIENIACZA	WERSJA OPROGRAM OWANIA UKŁADOWE GO BIBLIOTEKI	DODATKOW E BIBLIOTEKI W TEŚCIE	TYP STACJI TAŚM	WERSJA STEROWNIK A TAŚMY	WERSJA OPROGRAM OWANIA UKŁADOWE GO STACJI TAŚM
		1.8.0.11	3.47		HP 1760 LTO 4 HH SAS	1.0.6.1	U51U

Oracle StorageTek

NAZWA MODELU BIBLIOTEKI	SYSTEM OPERACYJNY	WERSJA STEROWNIKA ZMIENIACZA	WERSJA OPROGRAMO WANIA UKŁADOWEGO BIBLIOTEKI	TYP STACJI TAŚM	WERSJA STEROWNIKA TAŚMY	WERSJA OPROGRAMOW ANIA UKŁADOWEGO STACJI TAŚM
SL150			2.50	HP LTO5 HH FC		Y6IS
SL150			2.50	HP LTO5 HH SAS		Z6FS
SL150			2.50	HP LTO6 HH FC		25FS
SL150			2.50	HP LTO6 HH SAS		35FS
SL150			2.50	IBM LTO7 HH FC		G341
SL150-Tested			2.50	IBM LTO7 HH SAS		G341

System Center — wersje kompilacji Data Protection Manager

11.12.2019 • 2 minutes to read

W tym artykule opisano sposób określania bieżącego numeru wersji programu Microsoft System Center — Data Protection Manager i odpowiedniego pakietu zbiorczego aktualizacji. Każda wersja pakietu zbiorczego aktualizacji (UR) zawiera link do artykułu pomocy technicznej opisującego zmiany UR oraz linki do pobrania pakietu.

NOTE

Wszystkie pakiety zbiorcze aktualizacji programu System Center Data Protection Manager są zbiorcze. Oznacza to, że nie trzeba stosować URs w pożądanej kolejności. zawsze możesz zastosować najnowszą aktualizację. Jeśli wdrożono program System Center 2016 — Data Protection Manager i nigdy nie zastosowano pakietu zbiorczego aktualizacji, można rozpocząć instalację najnowszego.

Wersje kompilacji

W poniższej tabeli wymieniono wersje kompilacji dla Data Protection Manager 2016.

NUMER KOMPILACJI	BAZY	OPIS
4.3.1012.0	n/d	Data Protection Manager systemu Center 2016 Technical Preview
4.3.1071.0	n/d	System Center 2016 Technical Preview 2 Data Protection Manager
4.3.1043.0	n/d	System Center 2016 Technical Preview 3 Data Protection Manager
5.0.46.0	n/d	System Center 2016 Technical Preview 4 Data Protection Manager
5.0.58.0	n/d	System Center 2016 Technical Preview 5 Data Protection Manager
5.0.158.0	n/d	System Center 2016 Data Protection Manager RTM
5.0.247.0	3190600	Pakiet zbiorczy aktualizacji 1 dla programu System Center 2016 Data Protection Manager
5.0.322.0	3209593	Pakiet zbiorczy aktualizacji 2 dla programu System Center 2016 Data Protection Manager
5.0.342.0	4043316	Pakiet zbiorczy aktualizacji 4 dla programu System Center 2016 Data Protection Manager

NUMER KOMPILACJI	BAZY	OPIS
5.0.361.0	4090835	Pakiet zbiorczy aktualizacji 5 dla programu System Center 2016 Data Protection Manager
5.0.375.0	4456327	Pakiet zbiorczy aktualizacji 6 dla programu System Center 2016 Data Protection Manager

W poniższej tabeli wymieniono wersje kompilacji dla Data Protection Manager 1801.

NUMER KOMPILACJI	BAZY	OPIS
5.1.363.0	n/d	System Center 2016 1801

W poniższej tabeli wymieniono wersje kompilacji dla Data Protection Manager 1807.

NUMER KOMPILACJI	BAZY	OPIS
5.1.378.0	KB4339950	System Center 2016 1807

Następne kroki

[Co nowego w programie DPM](#)

Informacje o wersji programu System Center DPM

07.03.2020 • 37 minutes to read

W tym artykule wymieniono informacje o wersji programu System Center 2019 — Data Protection Manager (DPM).

W tym artykule wymieniono informacje o wersji programu System Center 1807 — Data Protection Manager (DPM).

W tym artykule wymieniono informacje o wersji programu System Center 1801 — Data Protection Manager (DPM).

W tym artykule wymieniono informacje o wersji programu System Center 2016 — Data Protection Manager (DPM).

Informacje o wersji programu DPM 2019

W poniższych sekcjach zestawiono informacje o wersji programu DPM 2019 i uwzględniono następujące znane problemy i rozwiązania.

Awaria konsoli programu DPM z powodu awarii usługi MSDPM

Opis: obecność zduplikowanych zadań zarządzania podsumowania, po uaktualnieniu programu DPM, może prowadzić do niepowodzenia wszystkich zadań w toku w godzinach od zera do awarii. W związku z tym można obserwować następujące kwestie:

- Replika jest niespójna.
- Przeładowanie magazynu spowodowany brakiem usunięć punktów odzyskiwania.
- Nieaktualne raporty programu DPM.
- Brak oczyszczenia dla historii zadań i zadań odzyskiwania pamięci.

Obejście:

1. Utwórz kopię zapasową bieżącego DPM database.
2. Otwórz program SQL Management Studio i Połącz się z wystąpieniem programu SQL hostującym DPMDB dla tego serwera.
3. Uruchom następujące zapytanie i sprawdź, czy zaplanowano co najmniej dwa zadania Menedżera podsumowania i zobacz, które starsze harmonogramy:

```
SELECT SCH.ScheduleId, SCH.JobDefinitionId, jd.CreationTime
FROM tbl_JM_JobDefinition JD
JOIN tbl_SCH_ScheduleDefinition SCH
ON JD.JobDefinitionId = SCH.JobDefinitionId
WHERE JD.Type = '282faac6-e3cb-4015-8c6d-4276fcc11d4'
AND JD.IsDeleted = 0
AND SCH.IsDeleted = 0
```

4. Jeśli została zwrócona więcej niż jeden wiersz, zrób wynikowe identyfikator harmonogramu ScheduleID i JobDefinitionID starszej pozycji i oznacz je jako usunięte.


```

update tbl_SCH_ScheduleDefinition
set IsDeleted = 1
where ScheduleId = 'ScheduleID '          --- Replace with Your ScheduleID
update dbo.tbl_JM_JobDefinition
set IsDeleted = 1
where JobDefinitionId = 'JobDefinitionID'  --- Replace with Your JobDefinitionID

```

5. Usuń zadanie SQL pasujące do identyfikator harmonogramu ScheduleID w obszarze Agent SQL Server — zadania. Po usunięciu zostanie rozwiązany awaria o godzinie zero.

Identyfikator harmonogramu ScheduleID to zadania SQL w ramach programu SQL Agent:

```

UPDATE MSDB.dbo.sysjobs
SET Enabled = 0
WHERE [Name] LIKE 'ScheduleID' --- Replace with Your ScheduleID

```

Maszyny wirtualne funkcji Hyper-V są dwukrotnie chronione podczas uaktualnienia maszyny wirtualnej

Opis: podczas uaktualniania maszyny wirtualnej funkcji Hyper-V z systemu windows Server 2012 R2 do systemu windows Server 2016 dwie wersje maszyny wirtualnej są wyświetlane w Kreatorze tworzenia grupy ochrony.

Obejście problemu: w przypadku chronionych maszyn wirtualnych, które mają zostać uaktualnione, przed uaktualnieniem maszyny wirtualnej należy zatrzymać ochronę z zachowaniem Zachowaj dane. Następnie Uaktualnij maszynę wirtualną i włącz ją ponownie w nowej grupie ochrony. Podczas konfigurowania ponownej ochrony wykonaj odświeżenie na hoście maszyny wirtualnej dla programu DPM w celu wykrycia uaktualnienia maszyny wirtualnej i Włącz ochronę go jako maszynę wirtualną RCT.

Przywrócenie poprzedniej wersji uaktualnionej maszyny wirtualnej funkcji Hyper-V powoduje niepowodzenie przyszłych punktów odzyskiwania

Opis: po uaktualnieniu chronionej maszyny wirtualnej funkcji Hyper-V 2012 R2 do wersji 2016, a następnie zatrzymaniu ochrony maszyny wirtualnej (ale zachowaniu danych), a następnie ponownym włączeniu ochrony, jeśli w oryginalnej lokalizacji zostanie odzyskana kopia 2012 R2, dalsze kopie zapasowe mogą zakończyć się niepowodzeniem.

Obejście: po odzyskaniu Zmień wersję maszyny wirtualnej na 2016, a następnie Uruchom sprawdzanie spójności.

Błędy ochrony odzyskiwania systemu od zera

Opis: w przypadku skonfigurowania ochrony przed odzyskiwaniem systemu od zera (BMR) zadanie ochrony BMR może zakończyć się niepowodzeniem z komunikatem, że rozmiar repliki nie jest wystarczająco duży.

Obejście: Użyj poniższej ścieżki rejestru, aby zmienić domyślny rozmiar repliki dla źródeł danych BMR. Otwórz Edytor rejestru i Zwiększ rozmiar repliki dla następującego klucza:

HKLM\Software\Microsoft\Microsoft Data Protection Manager\ConfigurationReplicaSizeInGBForSystemProtectionWithBMR (DWORD)

Zatrzymywanie DPM database ochrony w przypadku scenariuszy uaktualniania

Opis: podczas uaktualniania programu DPM Nazwa bazy danych może ulec zmianie w niektórych scenariuszach.

Obejście: w przypadku ochrony DPM Database upewnij się, że włączono ochronę nowej DPM Database. Po sprawdzeniu poprawności uaktualnienia programu DPM można usunąć ochronę poprzedniej DPM database.

RCT funkcji Hyper-V — niepowodzenie odzyskiwania jako plików kopii zapasowej D-T

Opis: odzyskiwanie maszyn wirtualnych RCT funkcji Hyper-V jako plików utworzonych bezpośrednio na taśmie (D-T) kończy się niepowodzeniem. Kopie zapasowe d-D-T nie wykazują tego problemu.

Obejście: Użyj odzyskiwania alternatywnej lokalizacji jako maszyny wirtualnej, a następnie przetransferuj te pliki

do odpowiedniej lokalizacji.

NOTE

Ta funkcja została rozwiązana w programie DPM 2019 UR1. Aby rozwiązać ten problem, można uaktualnić do programu DPM 2019 UR1 .

Program DPM 2019 nie obsługuje odzyskiwania użytkownika końcowego serwera plików z użyciem Nowoczesny magazyn kopii zapasowych (MB)

Opis: program DPM 2019 nie obsługuje odzyskiwania przez użytkownika końcowego z użyciem nowoczesny magazyn kopii zapasowych (MB).

Obejście: brak. Serwer plików EUR nie jest obsługiwany w przypadku korzystania z MB.

Serwery programu DPM 1801/1807 nie mogą być zarządzane przez konsolę centralną programu DPM 2019

Opis: w programie DPM 2019 Central Console nie można zarządzać wszystkimi serwerami programu DPM 1801 lub DPM 1807.

Obejście: Uaktualnij serwer programu DPM do wersji 2019.

Informacje o wersji programu DPM 1807

Aby wyświetlić listę błędów, które zostały rozwiązane w programie DPM 1807, zapoznaj się z [artykułem bazy wiedzy 4339950](#).

W wersji 1807 istnieją następujące problemy.

Maszyny wirtualne funkcji Hyper-V są dwukrotnie chronione podczas uaktualnienia maszyny wirtualnej

Opis: podczas uaktualniania maszyny wirtualnej funkcji Hyper-V z systemu windows Server 2012 R2 do systemu windows Server 2016 dwie wersje maszyny wirtualnej są wyświetlane w Kreatorze tworzenia grupy ochrony.

Obejście problemu: w przypadku maszyn wirtualnych, które nie zostały uaktualnione, Zatrzymaj ochronę przy zachowaniu danych. Uaktualnij maszynę wirtualną i Utwórz nową grupę ochrony. Następnie Odśwież źródła danych i Włącz ochronę maszyn wirtualnych. Po ponownym zastosowaniu ochrony maszyny wirtualne są chronione za pomocą Change Tracking odpornych na błędy (RCT).

Niepowodzenie instalacji agenta w systemie Windows Server 2008, Windows Server 2008 R2

Opis: w przypadku ochrony systemu windows Server 2008 lub windows Server 2008 R2 Instalacja agenta może zakończyć się niepowodzeniem.

Obejście: Uaktualnij program Windows Management Framework (WMF) na serwerze produkcyjnym do wersji 4.0. Pobierz pakiet WMF z programu <https://www.microsoft.com/download/details.aspx?id=40855>. Zainstaluj program WMF, a następnie zainstaluj agenta.

Przywrócenie poprzedniej wersji uaktualnionej maszyny wirtualnej funkcji Hyper-V spowoduje niepowodzenie przyszłych punktów odzyskiwania.

Opis: Jeśli uaktualnisz chronioną maszynę wirtualną funkcji Hyper-V 2012 R2 do wersji 2016, a następnie zatrzymasz ochronę maszyny wirtualnej (ale zachowasz dane), po czym ponownie włączysz ochronę, a następnie odzyskasz kopię wersji 2012 R2 w oryginalnej lokalizacji, wykonywanie dalszych kopii zapasowych może zakończyć się niepowodzeniem.

Obejście: po odzyskaniu Zmień wersję maszyny wirtualnej na 2016, a następnie Uruchom sprawdzanie spójności.

Błędy ochrony odzyskiwania systemu od zera

Opis: w przypadku skonfigurowania ochrony przed odzyskiwaniem systemu od zera (BMR) zadanie ochrony BMR może zakończyć się niepowodzeniem z komunikatem, że rozmiar repliki nie jest wystarczająco duży.

Obejście: Użyj poniższej ścieżki rejestru, aby zmienić domyślny rozmiar repliki dla źródeł danych BMR. Otwórz Edytor rejestru i Zwiększ rozmiar repliki dla następującego klucza:

HKLM\Software\Microsoft\Microsoft Data Protection Manager\ConfigurationReplicaSizeInGBForSystemProtectionWithBMR (DWORD)

Ponowne włączanie ochrony DPM database po uaktualnieniu do programu DPM 2016 lub 1801

Opis: po uaktualnieniu programu System center DPM 2012 R2 do wersji system center Data Protection Manager 2016 lub 1801 nazwa DPM Database może ulec zmianie w niektórych scenariuszach.

Obejście: w przypadku ochrony DPM Database upewnij się, że włączono ochronę nowej DPM Database. Po sprawdzeniu poprawności uaktualnienia programu DPM można usunąć ochronę starego DPM database.

Punkty odzyskiwania nie są czyszczone, co prowadzi do nagromadzenia punktów odzyskiwania

Opis: Program DPM oczyszcza punkty odzyskiwania starsze niż zakres przechowywania. Podczas oczyszczania program DPM oblicza Magazyn używany przez te punkty odzyskiwania do oczyszczenia. Wyczyszczanie opóźnień obliczeń magazynu.

Obejście problemu: Skonfiguruj program DPM, aby pominąć Obliczanie rozmiaru punktów odzyskiwania, które mają zostać oczyszczone. W związku z tym skrypt oczyszczający działa szybciej i oczyszcza wszystkie punkty odzyskiwania starsze niż zakres przechowywania, co uwalnia wszelkie wykorzystanie magazynu. Magazyn zużyty na źródło danych nie zostanie zaktualizowany do momentu zakończenia oczyszczania programu DPM. Użycie magazynu na wolumin nadal odzwierciedla poprawne wartości. Aby włączyć Obliczanie rozmiaru, Użyj skryptu programu PowerShell. Poniższy skrypt wykonuje obliczenia całkowitego rozmiaru.

Lokalizacja: Program Files\Microsoft System Center 2016\DPM\DPM\bin\Manage-DPMDSSStorageSizeUpdate.ps1

Skrypt:

```
Manage-DPMDSSStorageSizeUpdate.ps1 -ManageStorageInfo [StopSizeAutoUpdate | StartSizeAutoUpdate | GetSizeAutoUpdateStatus | UpdateSizeInfo ] [-UpdateSizeForDS <FilePath>] [-UpdatedDSSizeReport <FilePath>] [-FailedDSSizeUpdateFile <FilePath>]
```

- **ManageStorageInfo:** -określa rodzaj operacji.
 - **StopSizeAutoUpdate:** całkowicie zatrzymuje obliczenia rozmiaru. Rozmiary nie będą pokazywane zarówno w interfejsie użytkownika, jak i w programie PowerShell.
 - **StartSizeAutoUpdate:** przywraca obliczenia rozmiarów. Natychmiast po włączeniu obliczeń rozmiaru Użyj `UpdateSizeInfo` (w następujących opcjach), aby ponownie obliczyć rozmiary dla wszystkich źródeł danych, do których rozmiary raportowane w programie PowerShell i interfejsie użytkownika mogą być nieprawidłowe.
 - **GetSizeAutoUpdateStatus:** informuje, czy obliczenia rozmiarów są włączone.
 - **UpdateSizeInfo:** Wyzwała Obliczanie rozmiaru i zgłasza rozmiar używany przez źródło danych. Ponieważ może to być długotrwała operacja, należy używać jej tylko w razie potrzeby w scenariuszach takich jak rozliczenia. W tym czasie kopie zapasowe mogą zakończyć się niepowodzeniem z błędami instalacji dysku VHD.
- **UpdateSizeForDS:** ścieżka do pliku tekstowego z listą identyfikatorów źródeł danych, dla których ma zostać obliczony rozmiar. W każdym wierszu musi znajdować się parametr dataSourceID. Jeśli ta wartość nie zostanie przekazana, obliczanie rozmiaru zostanie wyzwolone dla wszystkich źródeł danych. Użyj po użyciu `UpdateSizeInfo` w `ManageStorageInfo`. Aby uzyskać identyfikatory DataSource określonych źródeł danych, użyj

```
Get-DPMProtectionGroup | Get-DPMDatasource | Format-table -Property Computer,name,ObjectType,Id .
```
- **UpdatedDSSizeReport:** Ścieżka do pliku, w którym są przechowywane zaktualizowane rozmiary źródeł

danych. Gdy nie przeszedł rozmiaru. csv, plik zostanie utworzony w katalogu wykonywania. Użyj po

`UpdateSizeInfo` w `ManageStorageInfo` .

- **FailedDSSizeUpdateFile:** ścieżka do pliku do przechowywania identyfikatorów źródeł danych, dla których nie można było obliczyć wykorzystania magazynu. Przyczyną może być na przykład trwające wykonywanie kopii zapasowych. Gdy ta wartość nie zostanie przekazana, w katalogu wykonywania zostanie utworzony plik failedDS.txt. Ten plik może zostać podany jako dane wejściowe dla opcji „UpdateSizeForDS” w celu zaktualizowania rozmiarów wszystkich źródeł danych. Powinno to być używane po użyciu `UpdateSizeInfo` w `ManageStorageInfo` .

RCT funkcji Hyper-V — niepowodzenie odzyskiwania jako plików kopii zapasowej D-T

Opis: odzyskiwanie maszyn wirtualnych RCT funkcji Hyper-V jako plików utworzonych bezpośrednio na taśmie (D-T) kończy się niepowodzeniem. D-D-T nie wykazuje tego problemu.

Obejście: Użyj odzyskiwania alternatywnej lokalizacji jako maszyny wirtualnej, a następnie przetransferuj te pliki do odpowiedniej lokalizacji.

Odzyskiwanie przez użytkownika końcowego serwera plików (EUR) nie jest dostępne w przypadku korzystania z Nowoczesny magazyn kopii zapasowych (MB)

Opis: w przypadku korzystania z nowoczesny magazyn kopii zapasowych (MB) z programem DPM 2016, odzyskiwanie przez użytkownika końcowego serwera plików jest niedostępne.

Obejście: brak. Serwer plików EUR nie jest obsługiwany w przypadku korzystania z MB.

Informacje o wersji programu DPM 1801

Następujące błędy zostały rozwiązane w wersji programu DPM 1801:

- Uaktualnienie agenta programu DPM na serwerze produkcyjnym spowoduje nieoczekiwane ponowne uruchomienie.
- Sprawdzanie spójności maszyn wirtualnych funkcji Hyper-V transferowa więcej danych niż rozmiar maszyn wirtualnych.

W wersji 1801 istnieją następujące problemy.

Instalacja dyskretna programu System Center DPM z programem SQL Server 2008

Opis: program DPM 2016 RTM nie zostanie zainstalowany w trybie dyskretnym na SQL Server 2008.

Obejście problemu: Wdróż program DPM 2016 RTM w wersji SQL Server nowszej niż 2008 lub użyj interfejsu użytkownika Instalatora programu DPM 2016.

Polecenie cmdlet Remove-DPMDiskStorage może usuwać woluminy z aktywnymi lub nieaktywnymi kopiami zapasowymi

Opis: Jeśli tworzone są kopie zapasowe źródeł danych woluminu (aktywnie lub w sposób aktywny), gdy polecenie cmdlet `Remove-DPMDiskStorage` jest używane do usuwania woluminów z programu DPM, źródła danych mogą być również usuwane.

Obejście: przed użyciem polecenia cmdlet do usuwania woluminów upewnij się, że źródła danych woluminu nie są używane (aktywnie lub w sposób aktywny).

Program DPM 2016 w systemie Windows Server 2016 zawiesza się

Opis: wykorzystanie pamięci na serwerze programu DPM stale wzrasta do momentu osiągnięcia 90%. Użycie pamięci spowalnia serwer programu DPM.

Obejście: Uaktualnij program DPM do programu DPM UR2 i zainstaluj [KB4013429](#) , aby rozwiązać ten problem.

Maszyny wirtualne funkcji Hyper-V są dwukrotnie chronione podczas uaktualnienia maszyny wirtualnej

Opis: podczas uaktualniania maszyny wirtualnej funkcji Hyper-V z systemu windows Server 2012 R2 do systemu windows Server 2016 dwie wersje maszyny wirtualnej są wyświetlane w Kreatorze tworzenia grupy ochrony.

Obejście problemu: w przypadku maszyn wirtualnych, które nie zostały uaktualnione, Zatrzymaj ochronę przy zachowaniu danych. Uaktualnij maszynę wirtualną i Utwórz nową grupę ochrony. Następnie Odśwież źródła danych i Włącz ochronę maszyn wirtualnych. Po ponownym zastosowaniu ochrony maszyny wirtualne są chronione za pomocą Change Tracking odpornych na błędy (RCT).

Niepowodzenie instalacji agenta w systemie Windows Server 2008, Windows Server 2008 R2

Opis: w przypadku ochrony systemu windows Server 2008 lub windows Server 2008 R2 Instalacja agenta może zakończyć się niepowodzeniem.

Obejście: Uaktualnij program Windows Management Framework (WMF) na serwerze produkcyjnym do wersji 4.0. Pobierz pakiet WMF z programu <https://www.microsoft.com/download/details.aspx?id=40855>. Zainstaluj program WMF, a następnie zainstaluj agenta.

Przywrócenie poprzedniej wersji uaktualnionej maszyny wirtualnej funkcji Hyper-V spowoduje niepowodzenie przyszłych punktów odzyskiwania.

Opis: Jeśli uaktualnisz chronioną maszynę wirtualną funkcji Hyper-V 2012 R2 do wersji 2016, a następnie zatrzymasz ochronę maszyny wirtualnej (ale zachowasz dane), po czym ponownie włączysz ochronę, a następnie odzyskasz kopię wersji 2012 R2 w oryginalnej lokalizacji, wykonywanie dalszych kopii zapasowych może zakończyć się niepowodzeniem.

Obejście: po odzyskaniu Zmień wersję maszyny wirtualnej na 2016, a następnie Uruchom sprawdzanie spójności.

Błędy ochrony odzyskiwania systemu od zera

Opis: w przypadku skonfigurowania ochrony przed odzyskiwaniem systemu od zera (BMR) zadanie ochrony BMR może zakończyć się niepowodzeniem z komunikatem, że rozmiar repliki nie jest wystarczająco duży.

Obejście: Użyj poniższej ścieżki rejestru, aby zmienić domyślny rozmiar repliki dla źródeł danych BMR. Otwórz Edytor rejestru i Zwiększ rozmiar repliki dla następującego klucza:

HKLM\Software\Microsoft\Microsoft Data Protection Manager\ConfigurationReplicaSizeInGBForSystemProtectionWithBMR (DWORD)

Ponowne włączanie ochrony DPM database po uaktualnieniu do programu DPM 2016

Opis: po uaktualnieniu programu System center DPM 2012 R2 do wersji system center Data Protection Manager 2016, nazwa DPM Database może ulec zmianie w niektórych scenariuszach.

Obejście: w przypadku ochrony DPM Database upewnij się, że włączono ochronę nowej DPM Database. Po sprawdzeniu poprawności uaktualnienia programu DPM można usunąć ochronę starego DPM database.

Punkty odzyskiwania nie są czyszczone, co prowadzi do nagromadzenia punktów odzyskiwania

Opis: Program DPM oczyszcza punkty odzyskiwania starsze niż zakres przechowywania. Podczas oczyszczania program DPM oblicza Magazyn używany przez te punkty odzyskiwania do oczyszczenia. Wyociszczanie opóźnień obliczeń magazynu.

Obejście problemu: Skonfiguruj program DPM, aby pominąć Obliczanie rozmiaru punktów odzyskiwania, które mają zostać oczyszczone. W związku z tym skrypt oczyszczający działa szybciej i oczyszcza wszystkie punkty odzyskiwania starsze niż zakres przechowywania, co uwalnia wszelkie wykorzystanie magazynu. Magazyn zużyty na źródło danych nie zostanie zaktualizowany do momentu zakończenia oczyszczania programu DPM. Użycie magazynu na wolumin nadal odzwierciedla poprawne wartości. Aby włączyć Obliczanie rozmiaru, Użyj skryptu programu PowerShell. Poniższy skrypt wykonuje obliczenia całkowitego rozmiaru.

Lokalizacja: Program Files\Microsoft System Center 2016\DPM\DPM\bin\Manage-DPMDStorageSizeUpdate.ps1

Skrypt:

```
Manage-DPMDSSStorageSizeUpdate.ps1 -ManageStorageInfo [StopSizeAutoUpdate | StartSizeAutoUpdate | GetSizeAutoUpdateStatus | UpdateSizeInfo ] [-UpdateSizeForDS <FilePath>] [-UpdatedDSSizeReport <FilePath>] [-FailedDSSizeUpdateFile <FilePath>]
```

- **ManageStorageInfo:** -określa rodzaj operacji.
 - **StopSizeAutoUpdate:** całkowicie zatrzymuje obliczenia rozmiaru. Rozmiary nie będą pokazywane zarówno w interfejsie użytkownika, jak i w programie PowerShell.
 - **StartSizeAutoUpdate:** przywraca obliczenia rozmiarów. Natychmiast po włączeniu obliczeń rozmiaru Użyj `UpdateSizeInfo` (w następujących opcjach), aby ponownie obliczyć rozmiary dla wszystkich źródeł danych, do których rozmiary raportowane w programie PowerShell i interfejsie użytkownika mogą być nieprawidłowe.
 - **GetSizeAutoUpdateStatus:** informuje, czy obliczenia rozmiarów są włączone.
 - **UpdateSizeInfo:** Wyzwala Obliczanie rozmiaru i zgłasza rozmiar używany przez źródło danych. Ponieważ może to być długotrwała operacja, należy używać jej tylko w razie potrzeby w scenariuszach takich jak rozliczenia. W tym czasie kopie zapasowe mogą zakończyć się niepowodzeniem z błędami instalacji dysku VHD.
- **UpdateSizeForDS:** ścieżka do pliku tekstowego z listą identyfikatorów źródeł danych, dla których ma zostać obliczony rozmiar. W każdym wierszu musi znajdować się parametr dataSourceID. Jeśli ta wartość nie zostanie przekazana, obliczanie rozmiaru zostanie wyzwolone dla wszystkich źródeł danych. Użyj po użyciu `UpdateSizeInfo` w `ManageStorageInfo`. Aby uzyskać identyfikatory DataSource określonych źródeł danych, użyj

```
Get-DPMPProtectionGroup | Get-DPMDatasource | Format-table -Property Computer,name,ObjectType,Id .
```
- **UpdatedDSSizeReport:** Ścieżka do pliku, w którym są przechowywane zaktualizowane rozmiary źródeł danych. Gdy nie przeszedł rozmiaru. csv, plik zostanie utworzony w katalogu wykonywania. Użyj po `UpdateSizeInfo` w `ManageStorageInfo`.
- **FailedDSSizeUpdateFile:** ścieżka do pliku do przechowywania identyfikatorów źródeł danych, dla których nie można było obliczyć wykorzystania magazynu. Przyczyną może być na przykład trwające wykonywanie kopii zapasowych. Gdy ta wartość nie zostanie przekazana, w katalogu wykonywania zostanie utworzony plik failedDS.txt. Ten plik może zostać podany jako dane wejściowe dla opcji „UpdateSizeForDS” w celu zaktualizowania rozmiarów wszystkich źródeł danych. Powinno to być używane po użyciu `UpdateSizeInfo` w `ManageStorageInfo`.

RCT funkcji Hyper-V — niepowodzenie odzyskiwania jako plików kopii zapasowej D-T

Opis: odzyskiwanie maszyn wirtualnych RCT funkcji Hyper-V jako plików utworzonych bezpośrednio na taśmie (D-T) kończyć się niepowodzeniem. W kopiach zapasowych D-D-T ten problem nie będzie występować.

Obejście: Użyj odzyskiwania alternatywnej lokalizacji jako maszyny wirtualnej, a następnie przetransferuj te pliki do odpowiedniej lokalizacji.

Odzyskiwanie przez użytkownika końcowego serwera plików (EUR) nie jest dostępne w przypadku korzystania z Nowoczesny magazyn kopii zapasowych (MB)

Opis: w przypadku korzystania z nowoczesny magazyn kopii zapasowych (MB) z programem DPM 2016, odzyskiwanie przez użytkownika końcowego serwera plików jest niedostępne.

Obejście: brak. Serwer plików EUR nie jest obsługiwany w przypadku korzystania z MB.

Błąd 4387 może pojawić się podczas instalowania programu DPM

Opis: podczas instalowania Data Protection Manager, gdy wprowadzasz wystąpienie SQL w **Data Protection Manager Instalatora > Sprawdzanie wymagań wstępnych >** wystąpienia pola tekstowego **programu SQL server**, może pojawić się błąd 4387.

Obejście: wykonaj wymagane akcje zgodnie z opisem w tym [artykule z bazy wiedzy](#) , a następnie spróbuj ponownie uruchomić Instalatora programu DPM.

Informacje o wersji programu System Center DPM 2016

Instalacja dyskretna programu System Center DPM z programem SQL Server 2008

Opis: program DPM 2016 RTM nie zostanie zainstalowany w trybie dyskretnym na SQL Server 2008.

Obejście problemu: Wdróż program DPM 2016 RTM w wersji SQL Server nowszej niż 2008 lub użyj interfejsu użytkownika Instalatora programu DPM 2016.

Polecenie cmdlet Remove-DPMDiskStorage może usuwać woluminy z aktywnymi lub nieaktywnymi kopiami zapasowymi

Opis: Jeśli tworzone są kopie zapasowe źródeł danych woluminu (aktywnie lub w sposób aktywny), gdy polecenie cmdlet [Remove-DPMDiskStorage](#) jest używane do usuwania woluminów z programu DPM, źródła danych mogą być również usuwane.

Obejście: przed użyciem polecenia cmdlet do usuwania woluminów upewnij się, że źródła danych woluminu nie są używane (aktywnie lub w sposób aktywny).

Program DPM 2016 w systemie Windows Server 2016 zawiesza się

Opis: wykorzystanie pamięci na serwerze programu DPM stale wzrasta do momentu osiągnięcia 90%. Użycie pamięci spowalnia serwer programu DPM.

Obejście: Uaktualnij program DPM do programu DPM UR2 i zainstaluj [KB4013429](#) , aby rozwiązać ten problem.

Maszyny wirtualne funkcji Hyper-V są dwukrotnie chronione podczas uaktualnienia maszyny wirtualnej

Opis: podczas uaktualniania maszyny wirtualnej funkcji Hyper-V z systemu windows Server 2012 R2 do systemu windows Server 2016 dwie wersje maszyny wirtualnej są wyświetlane w Kreatorze tworzenia grupy ochrony.

Obejście problemu: w przypadku maszyn wirtualnych, które nie zostały uaktualnione, Zatrzymaj ochronę przy zachowaniu danych. Uaktualnij maszynę wirtualną i Utwórz nową grupę ochrony. Następnie Odśwież źródła danych i Włącz ochronę maszyn wirtualnych. Po ponownym zastosowaniu ochrony maszyny wirtualne są chronione za pomocą Change Tracking odpornych na błędy (RCT).

Niepowodzenie instalacji agenta w systemie Windows Server 2008, Windows Server 2008 R2

Opis: w przypadku ochrony systemu windows Server 2008 lub windows Server 2008 R2 Instalacja agenta może zakończyć się niepowodzeniem.

Obejście: Uaktualnij program Windows Management Framework (WMF) na serwerze produkcyjnym do wersji 4.0. Pobierz pakiet WMF z programu <https://www.microsoft.com/download/details.aspx?id=40855>. Zainstaluj program WMF, a następnie zainstaluj agenta.

Przywrócenie poprzedniej wersji uaktualnionej maszyny wirtualnej funkcji Hyper-V spowoduje niepowodzenie przyszłych punktów odzyskiwania.

Opis: Jeśli uaktualnisz chronioną maszynę wirtualną funkcji Hyper-V 2012 R2 do wersji 2016, a następnie zatrzymasz ochronę maszyny wirtualnej (ale zachowasz dane), po czym ponownie włączysz ochronę, a następnie odzyskasz kopię wersji 2012 R2 w oryginalnej lokalizacji, wykonywanie dalszych kopii zapasowych może zakończyć się niepowodzeniem.

Obejście: po odzyskaniu Zmień wersję maszyny wirtualnej na 2016, a następnie Uruchom sprawdzanie spójności.

Błędy ochrony odzyskiwania systemu od zera

Opis: w przypadku skonfigurowania ochrony przed odzyskiwaniem systemu od zera (BMR) zadanie ochrony BMR może zakończyć się niepowodzeniem z komunikatem, że rozmiar repliki nie jest wystarczająco duży.

Obejście: Użyj poniższej ścieżki rejestru, aby zmienić domyślny rozmiar repliki dla źródeł danych BMR. Otwórz Edytor rejestru i Zwiększ rozmiar repliki dla następującego klucza:

HKLM\Software\Microsoft\Microsoft Data Protection Manager\ConfigurationReplicaSizeInGBForSystemProtectionWithBMR (DWORD)

Ponowne włączanie ochrony DPM database po uaktualnieniu do programu DPM 2016

Opis: po uaktualnieniu programu System center DPM 2012 R2 do wersji system center Data Protection Manager 2016, nazwa DPM Database może ulec zmianie w niektórych scenariuszach.

Obejście: w przypadku ochrony DPM Database upewnij się, że włączono ochronę nowej DPM Database. Po sprawdzeniu poprawności uaktualnienia programu DPM można usunąć ochronę starego DPM database.

Punkty odzyskiwania nie są czyszczone, co prowadzi do nagromadzenia punktów odzyskiwania

Opis: Program DPM oczyszcza punkty odzyskiwania starsze niż zakres przechowywania. Podczas oczyszczania program DPM oblicza Magazyn używany przez te punkty odzyskiwania do oczyszczenia. Wyczyszczenie opóźnień obliczeń magazynu.

Obejście problemu: Skonfiguruj program DPM, aby pominąć Obliczanie rozmiaru punktów odzyskiwania, które mają zostać oczyszczone. W związku z tym skrypt oczyszczający działa szybciej i oczyszcza wszystkie punkty odzyskiwania starsze niż zakres przechowywania, co uwalnia wszelkie wykorzystanie magazynu. Magazyn zużyty na źródło danych nie zostanie zaktualizowany do momentu zakończenia oczyszczania programu DPM. Użycie magazynu na wolumin nadal odzwierciedla poprawne wartości. Aby włączyć Obliczanie rozmiaru, Użyj skryptu programu PowerShell. Poniższy skrypt wykonuje obliczenia całkowitego rozmiaru.

Lokalizacja: Program Files\Microsoft System Center 2016\DPM\DPM\bin\Manage-
DPMDSStorageSizeUpdate.ps1

Skrypt:

```
Manage-DPMDSStorageSizeUpdate.ps1 -ManageStorageInfo [StopSizeAutoUpdate | StartSizeAutoUpdate |  
GetSizeAutoUpdateStatus | UpdateSizeInfo ] [-UpdateSizeForDS <FilePath>] [-UpdatedDSSizeReport <FilePath>] [-  
FailedDSSizeUpdateFile <FilePath>]
```

- **ManageStorageInfo:** -określa rodzaj operacji.
 - **StopSizeAutoUpdate:** całkowicie zatrzymuje obliczenia rozmiaru. Rozmiary nie będą pokazywane zarówno w interfejsie użytkownika, jak i w programie PowerShell.
 - **StartSizeAutoUpdate:** przywraca obliczenia rozmiarów. Natychmiast po włączeniu obliczeń rozmiaru Użyj `UpdateSizeInfo` (w następujących opcjach), aby ponownie obliczyć rozmiary dla wszystkich źródeł danych, do których rozmiary raportowane w programie PowerShell i interfejsie użytkownika mogą być nieprawidłowe.
 - **GetSizeAutoUpdateStatus:** informuje, czy obliczenia rozmiarów są włączone.
 - **UpdateSizeInfo:** Wyzwała Obliczanie rozmiaru i zgłasza rozmiar używany przez źródło danych. Ponieważ może to być długotrwała operacja, należy używać jej tylko w razie potrzeby w scenariuszach takich jak rozliczenia. W tym czasie kopie zapasowe mogą zakończyć się niepowodzeniem z błędami instalacji dysku VHD.
- **UpdateSizeForDS:** ścieżka do pliku tekstowego z listą identyfikatorów źródeł danych, dla których ma zostać obliczony rozmiar. W każdym wierszu musi znajdować się parametr dataSourceID. Jeśli ta wartość nie zostanie przekazana, obliczanie rozmiaru zostanie wyzwolone dla wszystkich źródeł danych. Użyj po użyciu `UpdateSizeInfo` w `ManageStorageInfo`. Aby uzyskać identyfikatory DataSource określonych źródeł danych, użyj

```
Get-DPMProtectionGroup | Get-DPMDatasource | Format-table -Property Computer,name,ObjectType,Id
```
- **UpdatedDSSizeReport:** Ścieżka do pliku, w którym są przechowywane zaktualizowane rozmiary źródeł

danych. Gdy nie przeszedł rozmiaru. csv, plik zostanie utworzony w katalogu wykonywania. Użyj po

`UpdateSizeInfo` w `ManageStorageInfo` .

- **FailedDSSizeUpdateFile:** ścieżka do pliku do przechowywania identyfikatorów źródeł danych, dla których nie można było obliczyć wykorzystania magazynu. Przyczyną może być na przykład trwające wykonywanie kopii zapasowych. Gdy ta wartość nie zostanie przekazana, w katalogu wykonywania zostanie utworzony plik failedDS.txt. Ten plik może zostać podany jako dane wejściowe dla opcji „UpdateSizeForDS” w celu zaktualizowania rozmiarów wszystkich źródeł danych. Powinno to być używane po użyciu `UpdateSizeInfo` w `ManageStorageInfo` .

RCT funkcji Hyper-V — niepowodzenie odzyskiwania jako plików kopii zapasowej D-T

Opis: odzyskiwanie maszyn wirtualnych RCT funkcji Hyper-V jako plików utworzonych bezpośrednio na taśmie (D-T) kończy się niepowodzeniem. W kopiach zapasowych D-D-T ten problem nie będzie występować.

Obejście: Użyj odzyskiwania alternatywnej lokalizacji jako maszyny wirtualnej, a następnie przetransferuj te pliki do odpowiedniej lokalizacji.

Odzyskiwanie przez użytkownika końcowego serwera plików (EUR) nie jest dostępne w przypadku korzystania z Nowoczesny magazyn kopii zapasowych (MB)

Opis: w przypadku korzystania z nowoczesny magazyn kopii zapasowych (MB) z programem DPM 2016, odzyskiwanie przez użytkownika końcowego serwera plików jest niedostępne.

Obejście: brak. Serwer plików EUR nie jest obsługiwany w przypadku korzystania z MB.

Błąd 4387 może pojawić się podczas instalowania programu DPM

Opis: podczas instalowania Data Protection Manager, gdy wprowadzasz wystąpienie SQL w **Data Protection Manager Instalatora > Sprawdzanie wymagań wstępnych >** wystąpienia pola tekstowego **programu SQL server** , może pojawić się błąd 4387.

Obejście: wykonaj wymagane akcje zgodnie z opisem w tym [artykule z bazy wiedzy](#) , a następnie spróbuj ponownie uruchomić Instalatora programu DPM.

Następne kroki

- Aby zainstalować program DPM, zapoznaj się z artykułem [Instalowanie programu DPM](#).
- Jeśli chcesz zapoznać się z informacjami dotyczącymi planowania środowiska, zobacz [Przygotowywanie środowiska dla programu System Center Data Protection Manager](#).
- Zobacz te artykułów bazy wiedzy dotyczące problemów specyficznych dla systemu plików ReFS — [KB4016173](#), [KB4035951](#).

Co nowego w programie System Center Data Protection Manager

08.02.2020 • 27 minutes to read

W tym artykule opisano nowe funkcje obsługiwane w programie System Center 2019 i 2019 UR1-Data Protection Manager (DPM).

Program DPM 1807 to Najnowsza wersja z półrocznego kanału programu System Center. Program System Center Data Protection Manager (DPM) można zaktualizować do wersji 1807 tylko w programie DPM 1801. W przypadku uaktualniania do programu DPM 1807 Zobacz informacje o [wersji dla 1807](#).

Program System Center DPM 1801 udostępnia następujące nowe funkcje:

W programie System Center DPM 2016 dodano ulepszenia w trzech kluczowych obszarach: zabezpieczeń, wydajności pracy oraz wydajności magazynu. Funkcja Modern Backup Storage korzysta z ulepszeń w systemie Windows Server 2016, oszczędzając dzięki temu 30–40% miejsca do magazynowania. Oprócz oszczędzania miejsca można stworzyć informacje o wydajności magazynu i wydajności przy użyciu programu MB, aby tworzyć kopie zapasowe określonych obciążeń na określonych woluminach. Ulepszona wydajność programu DPM zmniejsza wymagania operacji we/wy do 70%, co spowodowało szybsze wykonywanie kopii zapasowych. Program DPM 2016 obsługuje maszyny wirtualne z osłoną.

Nowe funkcje w programie DPM 2019

W poniższych sekcjach znajdują się szczegółowe informacje o nowych funkcjach i aktualizacjach funkcji obsługiwanych w programie DPM 2019.

Obsługa systemu Windows Server 2019

Program DPM 2019 można zainstalować w systemach Windows Server 2019 i Windows Server 2016.

Obsługa programu SQL 2017 jako DPM database

Program DPM 2019 obsługuje jako bazę danych SQL 2017.

SQL Server można zainstalować na serwerze zdalnym lub na serwerze DPM. Przed zainstalowaniem programu DPM należy zainstalować i uruchomić bazę danych.

Obsługa nowszych kopii zapasowych obciążeń

W programie DPM 2019 można tworzyć kopie zapasowe nowszych wersji obciążeń, wymienione poniżej:

- Maszyny wirtualne funkcji Hyper-V 2019
- Windows Server 2019
- Exchange 2019
- SharePoint 2019
- VMWare [vSphere 6,7](#)
- System Center Virtual Machine Manager 2019. [Dowiedz się więcej](#).

Szybsze tworzenie kopii zapasowych przy użyciu magazynu warstwowego za pomocą dysków SSD

Program DPM 2016 wprowadził [nowoczesny magazyn kopii zapasowych](#), zwiększając wykorzystanie magazynu i wydajność. MB korzysta z systemu plików ReFS jako bazowego i jest przeznaczony do korzystania z magazynu hybrydowego, takiego jak magazyn warstwowy.

Aby osiągnąć skalę i wydajność, MB zaleca się użycie małego procentu (4% całkowitego magazynu) w przypadku

programu DPM 2019 jako woluminu warstwowego w połączeniu z magazynem dysk twardy programu DPM. Program DPM 2019 z magazynem warstwowym oferuje do 50-70% szybszych kopii zapasowych. [Dowiedz się więcej.](#)

Obsługa centralnego monitorowania

W przypadku programu DPM 2019 wszyscy klienci programu DPM (połączeni z platformą Azure) mogą korzystać z funkcji monitorowania centralnego, A rozwiązanie do monitorowania zapewniane przez Microsoft Azure Backup.

Można monitorować kopie zapasowe zarówno lokalnie, jak i w chmurze, korzystając z Log Analytics z centralną funkcją monitorowania. [Dowiedz się więcej.](#)

Kopia zapasowa VMware na taśmie

Do długoterminowego przechowywania danych kopii zapasowej programu VMware można teraz włączyć kopie zapasowe programu VMware na taśmie. Częstotliwość tworzenia kopii zapasowych można wybrać na podstawie zakresu przechowywania (co będzie różnić się od 1-99 lat) na stacjach taśm. Dane na stacjach taśm mogą być kompresowane i szyfrowane.

Program DPM 2019 obsługuje zarówno oryginalne odzyskiwanie lokalizacji (OLR), jak i odzyskiwanie do lokalizacji alternatywnej (ALR)) w celu przywrócenia chronionej maszyny wirtualnej. [Dowiedz się więcej.](#)

Równoległe kopie zapasowe VMWare

W przypadku programu DPM 2019 wszystkie kopie zapasowe maszyn wirtualnych VMWare w ramach jednej grupy ochrony są równoległe, co prowadzi do 25% szybszych kopii zapasowych maszyn wirtualnych.

W starszych wersjach programu DPM równoległe kopie zapasowe były wykonywane tylko w grupach ochrony. W przypadku programu DPM 2019 zadania replikacji różnicowej oprogramowania VMWare są uruchamiane równoległe. Domyślnie liczba zadań do uruchomienia równoległego jest ustawiona na 8. [Dowiedz się więcej.](#)

Nowe funkcje w programie DPM 2019 UR1

Zapoznaj się z następującymi sekcjami, aby uzyskać informacje o nowych funkcjach i aktualizacjach funkcji obsługiwanych w programie DPM 2019 UR1.

W przypadku problemów rozwiązanych w 2019 UR1 zapoznaj się z [artykułem z bazy wiedzy](#).

Obsługa woluminów ReFS i woluminów ReFS z włączoną funkcją deduplikacji

W programie DPM 2019 UR1 można tworzyć kopie zapasowe woluminów i obciążeń systemu plików ReFS wdrożonych na woluminie systemu plików ReFS. Można utworzyć kopię zapasową następujących obciążeń wdrożonych na woluminach systemu plików ReFS:

- **System operacyjny (64 bitowy)** : Windows Server 2019, 2016, 2012 R2, 2012.
- **SQL Server**: SQL Server 2019, SQL Server 2017, 2016.
- **Exchange**: Exchange 2019, 2016.
- **SharePoint**: SharePoint 2019, 2016 z NAJNOWSZYM dodatkiem SP.

NOTE

Tworzenie kopii zapasowych maszyn wirtualnych funkcji Hyper-V przechowywanych na woluminie systemu plików ReFS jest obsługiwane przez program DPM 2019 RTM.

Obsługa systemu Windows Server Core

Program DPM 2019 UR1 można zainstalować w systemie Windows Server Core 2019 i 2016.

NOTE

Instalacja agenta MARS w systemie Windows Server Core nie jest obsługiwana. W przypadku tego ograniczenia program DPM nie może zostać połączony z magazynem usługi Azure Recovery Services, gdy jest zainstalowany w systemie Windows Server Core.

Wykluczanie dysku dla kopii zapasowej maszyny wirtualnej VMware

Program DPM 2019 UR1 umożliwia wykluczenie określonego dysku z kopii zapasowej maszyny wirtualnej VMware. [Dowiedz się więcej](#).

Obsługa dodatkowej warstwy uwierzytelniania do usuwania kopii zapasowych online

W przypadku programu DPM 2019 UR1 dodatkowa warstwa uwierzytelniania jest dodawana do krytycznych operacji. Po *zatrzymaniu ochrony* przy użyciu operacji *usuwania danych* zostanie wyświetlony monit o wprowadzenie zabezpieczającego numeru PIN.

Nowy parametr polecenia cmdlet

Program DPM 2019 UR1 zawiera nowy parametr **[-FragmentationPercentage]**. Nowy parametr oblicza wartość procentową fragmentacji dla repliki i jest uwzględniona w poleceniu cmdlet **copy-DPMDatasourceReplica**.

Co nowego w programie DPM 1807

Program DPM 1807 zawiera wiele poprawek błędów, które zwiększają wydajność.

Aby wyświetlić listę poprawionych błędów i instrukcje dotyczące instalacji programu DPM 1807, zobacz [artykuł w bazie wiedzy 4339950](#).

Nowe funkcje w programie DPM 1801

Program System Center DPM 1801 obsługuje [Tworzenie kopii zapasowych i przywracanie maszyn wirtualnych VMware](#) oraz rozszerza zalety nowoczesny magazyn kopii zapasowych do kopii zapasowych programu VMware. Aby uzyskać szczegółowe informacje na temat tworzenia kopii zapasowych maszyn wirtualnych VMware, zobacz [ten artykuł](#).

- Do 50% oszczędności miejsca do magazynowania
- Trzy razy szybsze kopie zapasowe
- Obciążenie — koligacja woluminu

Nowe funkcje w programie DPM 2016

Następujące funkcje są nowe w programie DPM lub zostały udoskonalone specjalnie dla wersji DPM 2016.

- **Nowoczesny magazyn kopii zapasowych** — używanie technologii systemowej systemu plików ReFS w celu przechowywania przyrostowych kopii zapasowych, program DPM 2016 zwiększa wykorzystanie magazynu i wydajność. Magazyn kopii zapasowych zwiększa się i zmniejsza w środowisku produkcyjnym. Nie istnieje nadmierna alokacja magazynu.
- **Śledzenie zmian odporne na błędy (RCT)** — program DPM korzysta z RCT (natywne śledzenie zmian w funkcji Hyper-V), co eliminuje konieczność czasochłonnych kontroli spójności. Śledzenie RCT zapewnia większą odporność niż śledzenie zmian w opartych na migawkach kopiach zapasowych usługi VSS. Program DPM używa również śledzenia RCT w przypadku przyrostowych kopii zapasowych. Dzięki temu identyfikuje zmiany dysku VHD na maszynach wirtualnych i transferuje tylko te bloki, które są wskazywane przez śledzenie zmian.

- **Ciągła ochrona podczas aktualizacji typu cluster-aware** — system Windows Server 2016 jest dostarczany z aktualizacją aktualizacji systemu operacyjnego klastra, w której klaster można uaktualnić do systemu Windows Server 2016 bez wyłączania go. Podczas aktualizacji program DPM 2016 stale chroni maszyny wirtualne zgodnie z umową dotyczącą poziomu usługi tworzenia kopii zapasowej.
- **Kopie zapasowe maszyn wirtualnych z osłoną** — maszyny wirtualne z osłoną w systemie Windows Server 2016 pomagają chronić poufne maszyny wirtualne przed inspekcją, manipulacją i kradzieżą danych przez złośliwe oprogramowanie i złośliwych administratorów. Kopie zapasowe w programie DPM 2016 zachowują ochronę dostarczaną przez maszyny wirtualne z osłoną w celu zapewnienia możliwości bezproblemowego i bezpiecznego odzyskania.
- **Funkcja Hyper-v z Bezpośrednie miejsca do magazynowania** - programu DPM rozpoznaje i chroni maszyny wirtualne funkcji Hyper-v wdrożone w bezpośrednie miejsca do magazynowania, zapewniając bezproblemowe tworzenie kopii zapasowych i odzyskiwanie maszyn wirtualnych w scenariuszach rozagregowanych i wieloskładnikowych.
- **Funkcja Hyper-v z klastrem SOFS ReFS** — program DPM 2016 może tworzyć kopie zapasowe maszyn wirtualnych funkcji Hyper-v wdrożonych w klastrach SOFS opartych na systemie ReFS. Obsługiwane jest również wykonywanie i odzyskiwanie kopii zapasowej maszyn wirtualnych opartych na RCT oraz innych maszyn wirtualnych.
- **Uaktualnienie serwera produkcyjnego programu DPM do 2016 nie wymaga ponownego uruchomienia** — w przypadku uaktualnienia do programu DPM 2016 nie jest wymagane ponowne uruchomienie serwera produkcyjnego. Aby uniknąć ponownego uruchamiania serwera produkcyjnego, uaktualnienie do wersji DPM 2016 i uaktualnienie agenta programu DPM należy przeprowadzić na serwerach produkcyjnych. Dzięki temu kopie zapasowe są wykonywane w sposób ciągły, a użytkownik może uruchomić serwer produkcyjny w dogodnym dla siebie czasie.

Modern Backup Storage

Modern Backup Storage to funkcja oferująca między innymi następujące korzyści:

Większe oszczędności miejsca do magazynowania

Dzięki zastosowaniu technologii takich jak system plików ReFS funkcja Modern Backup Storage umożliwia zaoszczędzenie 30–40% miejsca do magazynowania. Korzystanie z woluminów w systemie plików ReFS i przechowywanie kopii zapasowych na dyskach VHDX oznacza, że menedżer dysków lokalnych nie nakłada żadnych ograniczeń i nie dochodzi do nadmiernego alokowania miejsca w magazynie. Stopień wykorzystania magazynu przez program DPM jest elastyczny: ilość zajmowanego miejsca zwiększa się i zmniejsza w zależności od zmian magazynu źródła danych.

Szybsze tworzenie kopii zapasowych

Program DPM 2016 używa klonowania bloków w celu przechowywania kopii zapasowych na woluminach sformatowanych w systemie plików ReFS. Zamiast korzystać z kopii przy zapisie w celu przechowywania kopii zapasowych (z czego korzysta funkcja VolSnap w programie DPM 2012 R2), klonowanie bloków w programie DPM 2016 wykorzystuje przydzielanie przy zapisie. Ta zmiana zwiększa liczbę operacji wejścia/wyjścia na sekundę, dzięki czemu kopie zapasowe są tworzone nawet o 70% szybciej.

Wybór woluminów dla źródła danych w celu zwiększenia wydajności magazynu

Funkcja magazynu obsługującego obciążenia programu DPM zmniejsza koszty, zapewniając elastyczne opcje magazynu dla danego źródła danych. Oznacza to, że w celu wykonywania kopii zapasowych obciążeń o dużej liczbie operacji wejścia/wyjścia na sekundę program DPM może używać drogich dysków o wysokiej wydajności, takich jak dysków programu SQL lub SharePoint. W przypadku obciążeń o mniejszej liczbie operacji wejścia/wyjścia na sekundę mogą być używane magazyny o niższej wydajności.

Wykorzystanie magazynu kopii zapasowych odbywa się w zgodzie z produkcyjnym źródłem danych

Brak ograniczeń menedżera dysków logicznych (LDM) sprawia, że źródła danych rosną i zmniejszają się zgodnie z potrzebami, bez konieczności ręcznej interwencji. Program DPM nie musi z góry przydzielać miejsca w magazynie do źródeł danych i może pozwolić na dynamiczne dostosowywanie kopii zapasowych, osiągając w ten sposób wyższą wydajność przy mniejszym zapotrzebowaniu na miejsce w magazynie.

Ulepszenia ochrony zapewnianej przez funkcję Hyper-V

Poniższe informacje dotyczą ulepszeń w zakresie ochrony maszyn wirtualnych za pomocą programu DPM 2016.

Śledzenie zmian odporne na błędy (RCT)

W systemie Windows Server 2016 wirtualne dyski twarde funkcji Hyper-V mają wbudowaną funkcję śledzenia zmian. W efekcie w przypadku awarii hosta lub migracji maszyny wirtualnej śledzenie zmian jest automatycznie zachowywane. Dzięki RCT kopie zapasowe:

- **są bardziej niezawodne:** sprawdzanie spójności nie jest wymagane po migracji maszyny wirtualnej;
- **są skalowalne:** możliwość równoległego tworzenia większej liczby kopii zapasowych i mniejszy narzut na przechowywanie;
- **mają większą wydajność:** mniejszy wpływ na sieć szkieletową produkcji i szybsze wykonywanie kopii zapasowych.

Włączanie tworzenia kopii zapasowych maszyn wirtualnych z użyciem śledzenia zmian odpornego na błędy (RCT)

Maszyny wirtualne funkcji Hyper-V wdrożone w systemie Windows Server 2016 i chronione za pomocą programu DPM 2016 są domyślnie objęte śledzeniem zmian odpornym na błędy (RCT). Maszyny wirtualne wdrożone w systemie Windows Server 2012 R2 lub starszym nie obsługują funkcji RCT. Jednak starsze maszyny wirtualne można uaktualnić. Aby uaktualnić starsze maszyny wirtualne i umożliwić im obsługę funkcji RCT:

1. W menedżerze funkcji Hyper-V zamknij maszynę wirtualną.
2. W Menedżerze funkcji Hyper-V wybierz pozycję **akcja** > **wersja konfiguracji uaktualnienia**.

Jeśli ta opcja jest niedostępna dla konkretnej maszyny wirtualnej, oznacza to, że jest to już najwyższa wersja konfiguracji obsługiwana przez hosta funkcji Hyper-V. Aby uzyskać dodatkowe informacje dotyczące sprawdzania lub uaktualniania wersji konfiguracji maszyny wirtualnej, zobacz artykuł [Uaktualnianie maszyny wirtualnej do wersji dla systemu Windows Server 2016](#).

Jeśli chcesz uaktualnić konfigurację maszyny wirtualnej przy użyciu programu Windows PowerShell, uruchom następujące polecenie, gdzie vmname to nazwa maszyny wirtualnej.

```
Update-VMVersion <vmname>
```

3. Na serwerze programu DPM 2016:

- Zatrzymaj ochronę maszyny wirtualnej, a następnie wybierz pozycję **Zachowaj dane**.
- W konsoli administratora programu DPM 2016 kliknij pozycję **Ochrona** na wstążce narzędzi, a następnie kliknij pozycję **Nowe**, aby uruchomić kreatora tworzenia ochrony. Wykonaj kroki w kreatorze, a następnie wybierz pozycję **Odśwież**, aby zaktualizować źródła danych.
- Wybierz maszynę wirtualną i utwórz nową grupę ochrony.
- Po wygaśnięciu zakresu przechowywania usuń zachowane dane starej maszyny wirtualnej.

Powyższa procedura służy do tworzenia kopii zapasowych obsługujących RCT maszyn wirtualnych wdrożonych w różnych konfiguracjach. W poniższych sekcjach opisano obsługiwane scenariusze:

Spełnienie postanowień umowy SLA dla usługi kopia zapasowa podczas stopniowego uaktualnienia systemu operacyjnego klastra

Uaktualnienie stopniowe systemu operacyjnego klastra jest funkcją systemu Windows Server 2016, która służy do uaktualnienia systemu operacyjnego węzłów klastra z wersji Windows Server 2012 R2 do wersji Windows Server

2016 bez zatrzymywania obciążeń funkcji Hyper-V ani obciążeń serwera plików skalowalnego w poziomie (SOFS). Uaktualnienie stopniowe systemu operacyjnego klastra gwarantuje, że ochrona nie zostanie zakłócona podczas uaktualniania systemu operacyjnego. Taka nieprzerwana ochrona jest zgodna z postanowieniami umowy SLA dla usługi kopia zapasowa, sprzyja ciągłości działalności i zapewnia spokój administratorom kopii zapasowych. Szczegółowe informacje na temat stopniowego uaktualniania klastra systemu operacyjnego zawiera artykuł [Proces stopniowego uaktualniania klastra systemu operacyjnego](#).

Aby umożliwić nieprzerwaną ochronę, wykonaj następujące kroki dla każdego węzła:

1. Opróżnij role w węźle.

To spowoduje przełączenie węzła w stan wstrzymania i wywoła automatyczną migrację dowolnej maszyny wirtualnej znajdującej się w tym węźle do innego węzła klastra.

2. Uruchom ponownie węzeł.

3. Wyklucz węzeł.

4. Zainstaluj system Windows Server 2016.

5. Zainstaluj agenta programu DPM.

6. Dodaj węzeł z powrotem do klastra.

Dzięki temu możliwe będzie tworzenie kopii zapasowych bez sprawdzania spójności i z zachowaniem aktywności klastra.

Bezproblemowa ochrona i odzyskiwanie maszyn wirtualnych z osłonami (maszyny wirtualne obsługujące moduł vTPM)

Moduły TPM (Trusted Platform Module) to układy znajdujące się na płycie głównej komputerów. Pomagają one w integracji kluczy kryptograficznych. Te klucze są używane przez funkcję BitLocker do ochrony komputera, nawet jeśli zostanie skradziony. Wirtualny moduł TPM (vTPM) to funkcja systemu Windows Server 2016. Dzięki modułowi vTPM można korzystać z funkcji BitLocker oraz wirtualnego modułu TPM, aby szyfrować maszynę wirtualną, obejmując ją w ten sposób ochroną. Te maszyny wirtualne, nazywane maszynami wirtualnymi z osłoną, można uruchamiać tylko na hostach w dobrej kondycji i zatwierdzonych w sieci szkieletowej.

Program DPM 2016 obsługuje wykonywanie i odzyskiwanie kopii zapasowych maszyn wirtualnych z osłoną, których dyski VHD/VHDX są chronione przez moduł vTPM. Należy zauważyć, że w tym scenariuszu nie jest dostępne odzyskiwanie na poziomie elementu (ILR) ani odzyskiwanie do lokalizacji alternatywnej (ALR) do lokalizacji poza chronioną siecią szkieletową.

Ochrona maszyn wirtualnych przechowywanych w bezpośrednim miejscu do magazynowania

Bezpośrednie miejsca do magazynowania korzystają z funkcji miejsca do magazynowania, która została wprowadzona w systemie Windows Server 2012 R2, dzięki czemu możliwe jest wdrożenie systemów magazynów o wysokiej dostępności przy użyciu lokalnego magazynu. Bezpośrednie miejsca do magazynowania korzystają z dysków lokalnych na hostach, aby zapewnić współdzieloną pulę klastrowanych magazynów, które mogą służyć jako podstawowy magazyn dla plików maszyny wirtualnej funkcji Hyper-V lub jako zapasowy magazyn dla plików maszyny wirtualnej funkcji Hyper-V Replica. Głównym zastosowaniem bezpośrednich miejsc do magazynowania jest magazyn w chmurze prywatnej, lokalny w przypadku przedsiębiorstw lub w hostowanych chmurach prywatnych w przypadku dostawców usług. Aby uzyskać więcej informacji na temat bezpośrednich miejsc do magazynowania, zobacz artykuł [Bezpośrednie miejsca do magazynowania w systemie Windows Server 2016](#).

Program DPM zapewnia ochronę maszyn wirtualnych funkcji Hyper-V, które korzystają z bezpośredniego miejsca do magazynowania. Większość konfiguracji jest obsługiwanych — w tym również tworzenie kopii zapasowych maszyn wirtualnych [w scenariuszach hiper zbieżności bezpośredniego miejsca do magazynowania](#) — za pomocą składników funkcji Hyper-V (do obliczania) i bezpośredniego miejsca do magazynowania (do magazynowania) w tym samym klastrze. Pamiętaj, że wykonywanie kopii zapasowych i przywracanie maszyn wirtualnych działających w systemie Windows Nano Server nie jest obsługiwane.

Ochrona maszyn wirtualnych przechowywanych w klastrach SOFS opartych na systemie plików ReFS

Program DPM 2016 może tworzyć kopie zapasowe maszyn wirtualnych wdrożonych w klastrach SOFS opartych na systemie plików ReFS.

Aby chronić maszyny wirtualne w klastrach SOFS, dodaj następujące konta komputerów do grup operatorów kopii zapasowych oraz nadaj im prawa dostępu do udziału.

- W przypadku ochrony maszyny wirtualnej o wysokiej dostępności (HA) należy podać nazwę konta komputera klastra hosta i węzłów klastra, a także nazwę serwera programu DPM.
- W przypadku ochrony maszyn wirtualnych innych niż HA należy podać nazwę komputera hosta funkcji Hyper-V i nazwę serwera programu DPM.

Aby dodać konta komputerów do grupy operatorów kopii zapasowych, wykonaj następujące kroki dla każdego węzła w klastrze SOFS:

1. Otwórz wiersz polecenia i wpisz **lusrmgr.msc**, aby otworzyć okno dialogowe Użytkownicy i grupy lokalne.
2. W oknie dialogowym Użytkownicy i grupy lokalne kliknij pozycję **Grupy**.
3. Na liście grup kliknij prawym przyciskiem myszy pozycję **Operatorzy kopii zapasowych** i wybierz pozycję **Właściwości**.

Zostanie otwarte okno dialogowe **Właściwości operatorów kopii zapasowych**.

4. W oknie dialogowym **Właściwości operatorów kopii zapasowych** kliknij pozycję **Dodaj**.
5. W oknie dialogowym **Wybieranie użytkowników, komputerów, kont usług lub grup** kliknij pozycję **Typy obiektów**. Zostanie otwarte okno dialogowe **Typy obiektów**.
6. W oknie dialogowym **Typy obiektów** wybierz pozycję **Komputery** i kliknij przycisk **OK**. Okno dialogowe **Typy obiektów** zostanie zamknięte.
7. W oknie dialogowym **Wybieranie użytkowników, komputerów, kont usług lub grup** wprowadź nazwę serwera lub klastra, a następnie kliknij pozycję **Sprawdź nazwy**.
8. Po zidentyfikowaniu komputerów należy ponownie uruchomić węzeł.

Aby udzielić uprawnień dostępu do udziału

1. Na serwerze, na którym jest hostowany udział SOFS/SMB, Otwórz **Menedżer serwera > usługi plików i magazynowania > udziały**.
2. Kliknij prawym przyciskiem myszy udział magazynu maszyny wirtualnej, a następnie kliknij pozycję **Właściwości**.
3. W oknie dialogowym **Właściwości**, w menu nawigacji z lewej strony, kliknij pozycję **Uprawnienia**.
4. Kliknij pozycję **Dostosowywanie uprawnień**, aby otworzyć okno dialogowe Zaawansowane ustawienia zabezpieczeń.
5. Na karcie **Uprawnienia** kliknij pozycję **Dodaj**.
6. Kliknij pozycję **Wybierz podmiot zabezpieczeń**.
7. W oknie dialogowym **Wybieranie użytkowników, komputerów, kont usług lub grup** kliknij pozycję **Typy obiektów**.
8. W oknie dialogowym **Typy obiektów** wybierz pozycję **Komputery** i kliknij przycisk **OK**.
9. W oknie dialogowym **Wybieranie użytkowników, komputerów, kont usług lub grup** wprowadź nazwę węzła lub klastra funkcji Hyper-V, do którego chcesz posiadać uprawnienia.
10. Kliknij przycisk **Sprawdź nazwy**, aby rozpoznać nazwę, a następnie kliknij przycisk **OK**.

11. W oknie dialogowym **Wpis uprawnień dla udziału** wybierz pozycję **Pełna kontrola** i kliknij przycisk **OK**.
12. W oknie dialogowym **Zaawansowane ustawienia zabezpieczeń dla udziału** kliknij kartę **Udział** i powtórz kroki od 6 do 11 dla karty **Udział** zamiast dla karty **Uprawnienia**.
13. Po zakończeniu dodawania uprawnień dla serwerów kliknij przycisk **Zastosuj**.

Wykonanie tych kroków przygotowuje maszyny wirtualne w udziałach SOFS do procesu tworzenia kopii zapasowej.

Następne kroki

- [Instalowanie programu DPM](#)
- [Uaktualnianie instalacji programu DPM](#)

What's supported and what isn't for DPM?

(Elementy obsługiwane i nieobsługiwane przez program DPM)

14.02.2020 • 29 minutes to read

Ten temat zawiera podsumowanie typowych informacji pomocy technicznej, które mogą być potrzebne podczas wdrażania i konserwacji programu System Center — Data Protection Manager.

Problemy związane z instalacją i wdrożeniem

Opcje wdrożenia programu DPM

Problem: Program DPM można instalować w środowiskach fizycznych i wirtualnych.

Więcej informacji: program DPM można zainstalować w następujący sposób:

- Jako autonomiczny serwer fizyczny — programu DPM nie można wdrożyć w klastrze fizycznym, ale można zarządzać wieloma serwerami DPM z jednej lokalizacji za pomocą konsoli centralnej w programie Operations Manager.
- Jako lokalną maszynę wirtualną — program DPM można wdrożyć jako maszynę wirtualną funkcji Hyper-V: jako pojedynczy serwer lub klaster maszyn wirtualnych. Program DPM instaluje się tak samo, jak w przypadku instalacji fizycznej. Aby uzyskać szczegółowe informacje, zobacz wiersz [Program DPM instalowany jako maszyna wirtualna funkcji Hyper-V](#) w tabeli wymagań wstępnych dotyczących instalacji.
- Jako maszynę wirtualną platformy Azure — od programu DPM 2012 R2 z aktualizacją 3 można zainstalować program DPM jako maszynę wirtualną platformy Azure. Takie wdrożenie podlega kilku ograniczeniom. Aby uzyskać szczegółowe informacje, zobacz wiersz [programu DPM jako maszynę wirtualną platformy Azure](#) w tabeli wymagań wstępnych Instalatora.
- Jako maszynę wirtualną programu VMWare — od programu DPM 2012 R2 z aktualizacją 5 można zainstalować program DPM na maszynie wirtualnej systemu Windows w środowisku programu VMWare. W takiej konfiguracji program DPM może chronić obciążenia serwera firmy Microsoft, uruchomione jako maszyny wirtualne systemu Windows w środowisku programu VMWare.

Współużytkowanie biblioteki przez różne wersje programu DPM nie jest obsługiwane

Problem: różne wersje programu DPM (na przykład DPM 2012 R2 i DPM 2016) nie mogą działać jako klienci korzystający z tej samej biblioteki.

Obejście: brak. Wszystkie serwery DPM korzystające z jednej biblioteki udostępnionej muszą mieć zainstalowaną tę samą wersję programu DPM.

Uaktualnianie programu System Center 2010 bezpośrednio do wersji System Center 2016 nie jest obsługiwane

Problem: Uaktualnianie nie jest obsługiwane.

Obejście problemu: Najpierw musisz przeprowadzić uaktualnienie do wersji DPM 2012 R2.

Program DPM nie działa w tureckiej wersji językowej systemów operacyjnych Windows 2012

Problem: Brak obsługi języka

Obejście: Brak

Programu DPM w wersji 2010 lub nowszej nie można uruchomić na serwerze z 32-bitowym systemem operacyjnym

Problem: Ograniczenie systemu operacyjnego.

Obejście problemu: Program należy instalować wyłącznie na serwerach z systemem 64-bitowym. Aby zapoznać się z pełną listą wymagań systemowych, zobacz [Przygotowywanie środowiska dla programu System Center Data Protection Manager](#).

Znak podkreślenia w nazwie serwera programu SQL Server nie jest obsługiwany

Problem: Jeśli nazwa zdalnego serwera SQL wskazanego podczas instalacji programu DPM zawiera znak podkreślenia, instalacja może zakończyć się niepowodzeniem.

Obejście: określ nazwę SQL Server, która nie zawiera znaku podkreślenia .

Kompresja NTFS nie jest obsługiwana na woluminach programu DPM

Problem: Kompresja NTFS nie jest obsługiwana.

Obejście: Brak

Zmiana nazwy serwera programu DPM nie jest obsługiwana

Problem: Zmiana nazwy nie jest obsługiwana.

Obejście: Brak

Przenoszenie serwera programu DPM do innej domeny nie jest obsługiwane

Problem: Przenoszenie serwera programu DPM do innej domeny po wdrożeniu nie jest obsługiwane.

Obejście: Brak

Program DPM na kontrolerze domeny może chronić tylko lokalne źródła danych

Problem: To wdrożenie nie jest obsługiwane.

Obejście problemu: Jeśli chcesz zainstalować agenta ochrony programu DPM na innych komputerach, aby je chronić, nie instaluj programu DPM na kontrolerze domeny.

Program DPM nie może korzystać z programu SQL Server uruchomionego na kontrolerze domeny

Problem: Wdrożenie bazy danych nie jest obsługiwane.

Obejście problemu: Jeśli chcesz użyć zdalnego wystąpienia programu SQL Server jako bazy danych programu DPM, upewnij się, że to wystąpienie programu SQL Server nie jest uruchomione na kontrolerze domeny.

Nie można zainstalować programu DPM 2016 w programie SQL 2016 z dodatkiem SP1 (lub nowszym)

Problem: Instalacja w programie SQL 2016 z dodatkiem SP1 (lub nowszym) nie jest obsługiwana.

Obejście: brak.

Przenoszenie chronionych serwerów z wykorzystaniem serwerów pomocniczych programu DPM

Przenoszenie chronionych serwerów między serwerami programu DPM, które są objęte ochroną pomocniczą, nie jest obsługiwane. Za ilustrację może służyć następujący przykład:

- Serwer1
- Serwer2
- DPM1 działający jako podstawowy serwer DPM
- DPM2 działający jako inny podstawowy serwer DPM
- DPM3 działający jako serwer pomocniczy dla DPM1 i DPM2

Gdzie:

- Serwer1 jest chroniony przez DPM1
- Serwer2 jest chroniony przez DPM2
- DPM3 jest serwerem pomocniczym dla DPM1 i DPM2 (i w związku z tym chroni Serwer1 i Serwer2).

Założmy następujące sytuacje:

- **Scenariusz 1**

- Serwer DPM1 uległ awarii lub został usunięty z infrastruktury.
- Chcesz teraz chronić Serwer1 za pomocą DPM2 (z DPM3 działającym jako serwer pomocniczy).

- **Scenariusz 2**

- Serwer DPM1 uległ awarii lub został usunięty z infrastruktury.
- Chcesz teraz chronić Serwer1 za pomocą DPM3.

Żaden z tych scenariuszy nie jest obsługiwany. Możesz wybrać tylko jedną z następujących opcji:

- **Opcja 1** — użyć opcji „Przełącz ochronę” na DPM3 dla komputera Serwer1 i pozostawić DPM3 działający w tym trybie. Zauważ, że w tym scenariuszu nie można dodać dodatkowej ochrony komputera Serwer1 na innym serwerze DPM podczas korzystania z trybu przełączonej ochrony.
- **Opcja 2** — odbudować DPM1 o takiej samej nazwie i przywrócić bazę danych programu DPM. Pozwoli to wznowić ochronę podstawową przez program DPM.
- **Opcja 3** — przenieść ochronę komputera Serwer1 na nowy serwer DPM (DPM4), który nie jest związany z DPM3.

Problemy związane z magazynowaniem

Odwołania do starych bibliotek taśm nie są usuwane z bazy danych programu DPM

Problem: Przestarzałe biblioteki taśm wciąż znajdują się na listach w poleceniach cmdlet programu PowerShell w programie DPM, na przykład get-dpmlibrary.

Obejście: Brak

Obsługa wirtualnej biblioteki taśm

Problem: Czy wirtualne biblioteki taśm są obsługiwane?

Obejście problemu: Wirtualne biblioteki taśm skonfigurowane z wirtualną kartą Fibre Channel są obsługiwane tylko w przypadku uruchomienia programu Data Protection Manager 2012 R2 UR3 lub nowszego na certyfikowanym sprzęcie. Aby uzyskać bieżącą listę obsługiwanego sprzętu, [zobacz zgodne biblioteki taśm dla programu System Center DPM 2012 i nowszych](#). Aby sprawdzić, czy dana biblioteka taśm jest obsługiwana przez wirtualną kartę Fibre Channel, skontaktuj się z dostawcą sprzętu taśm i poproś o [sprawdzanie zgodności biblioteki taśm](#).

Nie można używać dysków USB i dysków wymiennych w puli magazynów programu DPM

Problem: Dyski USB i magazyny wymienne, na przykład w standardzie Firewire.

Obejście: brak. Przyczyną braku obsługi jest ograniczenie dotyczące dysków dynamicznych w systemie Windows.

Dane na udostępnionych woluminach klastra (CSV)

Problem: Program DPM obsługuje wyłącznie ochronę maszyn wirtualnych funkcji Hyper-V na udostępnionych

woluminach klastra (CSV). Ochrona innych obciążeń znajdujących się na woluminach CSV nie jest obsługiwana.

Obejście: brak.

Problemy z deduplikacją

Obsługa woluminów z deduplikacją

Problem: Obsługa deduplikacji w programie DPM zależy od jej obsługi w systemie operacyjnym.

W przypadku woluminów NTFS:

SYSTEM OPERACYJNY SERWERA CHRONIONEGO	SYSTEM OPERACYJNY SERWERA PROGRAMU DPM	WERSJA PROGRAMU DPM	OBSŁUGA DEDUPLIKACJI
Windows 2012	Windows Server 2012	DPM 2012 z dodatkiem SP1, DPM 2012 R2	T
Windows 2012	Windows Server 2012 R2	DPM 2012 R2	T
Windows Server 2012 R2	Windows Server 2012 R2	DPM 2012 R2	T
Windows Server 2012 R2	Windows Server 2012	DPM 2012 z dodatkiem SP1, DPM 2012 R2	N

Woluminy systemu plików ReFS:

NOTE

Program DPM 2019 UR1 obsługuje ochronę woluminów ReFS z deduplikacją.

SYSTEM OPERACYJNY SERWERA CHRONIONEGO	SYSTEM OPERACYJNY SERWERA PROGRAMU DPM	WERSJA PROGRAMU DPM	OBSŁUGA DEDUPLIKACJI
Windows Server 2012, 2012 R2, 2016 i 2019	Windows Server 2016, 2019	UR1 PROGRAMU DPM 2019	T

Obejście problemu: Używaj zgodnie z ograniczeniami w obsłudze.

Deduplikacja w systemie Windows może nie być obsługiwana na woluminach, na których znajdują się pliki VHD lub VHDX

Problem: Obsługa deduplikacji

Obejście problemu: Wdróż program DPM jako maszynę wirtualną.

Deduplikację magazynu programu DPM możesz włączyć, jeśli jest on uruchomiony na maszynie wirtualnej funkcji Hyper-V, i przechowywać dane kopii zapasowej w plikach VHD w folderach udostępnionych na serwerach plików systemu Windows z włączoną deduplikacją danych. Więcej informacji na temat tego scenariusza znajduje się w temacie [Deduplikacja magazynu programu DPM](#).

Nie można chronić systemu plików z deduplikacją przy użyciu pomocniczego serwera programu DPM

Problem: Jeśli system plików z deduplikacją jest chroniony przez podstawowy serwer DPM, nie można chronić go przy użyciu pomocniczego serwera DPM.

Obejście: brak.

Odzyskiwanie na poziomie elementu nie jest obsługiwane

Problem: Jeśli chronisz maszyny wirtualne zawierające woluminy z deduplikacją, wykonanie odzyskiwania na poziomie elementu z tych plików VHD/VHDX nie jest możliwe.

Obejście problemu: Przywróć plik VHD/VHDX zawierający wolumin z deduplikacją na serwer z systemem Windows 2012 R2, na którym jest zainstalowana rola Deduplikacja danych. Zainstaluj plik VHD w przystawce Zarządzanie dyskami i skopiuj z niego potrzebne pliki.

Problemy związane z ochroną klientów i serwerów

Parametry obsługi ochrony komputerów z systemami operacyjnymi klienta w programie DPM

Problem: Obsługiwane są następujące scenariusze ochrony:

- Windows 8.1 klienci mogą być chronieni przy użyciu programu DPM 2012 R2 i DPM 2016.
- Komputery z systemem Windows 7 mogą być chronione przy użyciu programu DPM 2012 R2 i DPM 2016.

Obejście problemu: Upewnij się, że korzystasz z właściwej wersji programu DPM.

Obsługa ochrony komputerów z systemami operacyjnymi serwera za pomocą programu DPM

Problem: Obsługiwane są następujące scenariusze ochrony:

- System Windows Server 2012 R2 można chronić przy użyciu programu DPM 2012 R2 lub nowszego.
- Systemy Windows Server 2012 lub 2012 z dodatkiem SP1 mogą być chronione przy użyciu programu DPM 2012 R2 lub nowszego.
- System Windows Server 2008 R2 z dodatkiem SP1 systemu Windows Server 2008 R2 można chronić przy użyciu programu DPM 2012 R2 i DPM 2016.
- Systemy Windows Server 2008 i Storage Server 2008 mogą być chronione przy użyciu programu DPM 2012 R2 z [pakietem zbiorczym aktualizacji 2](#) i programem DPM 2016.

Obejście problemu: Upewnij się, że korzystasz z właściwej wersji programu DPM.

Przy użyciu programu DPM nie można chronić udziałów na serwerach plików skalowalnych w poziomie (SOFS)

Problem: Przy użyciu programu DPM nie można chronić udziałów na serwerach SOFS.

Obejście problemu: Upewnij się, że udziały, które chcesz chronić, nie znajdują się na serwerach SOFS.

Problemy z serwerem plików

Odzyskiwanie przez użytkownika końcowego serwera plików (EUR) nie jest dostępne w przypadku korzystania z Nowoczesny magazyn kopii zapasowych (MB)

Opis: jeśli używasz nowoczesny magazyn kopii zapasowych (MB) z programem DPM 2016 lub nowszym, odzyskiwanie przez użytkownika końcowego serwera plików jest niedostępne.

Obejście: brak. Serwer plików EUR nie jest obsługiwany w przypadku korzystania z MB.

Problemy związane z ochroną danych

Program DPM nie tworzy kopii zapasowej udostępnionego dysku VHDX

Problem: program DPM nie może tworzyć kopii zapasowych maszyn wirtualnych przy użyciu udostępnionych dysków (które są potencjalnie dołączone do innych maszyn wirtualnych), ponieważ składnik zapisywania usługi VSS funkcji Hyper-V nie może tworzyć kopii zapasowych woluminów, których kopię zapasową utworzono

Obejście: aby uniknąć utraty danych, użyj innej metody, aby utworzyć kopię zapasową danych na wirtualnym

dysku VHD.

Ochrona danych może nie działać, gdy zmieni się ścieżka źródła danych

Problem: Podczas ochrony folderu udostępnionego ścieżka do tego folderu uwzględnia ścieżkę logiczną na woluminie. Jeśli folder udostępniony zostanie przeniesiony, ochrona zakończy się niepowodzeniem. Ponadto jeśli nowa, zmieniona ścieżka pliku chronionego źródła danych na woluminie wykorzystującym system szyfrowania plików (EFS) jest dłuższa niż 5120 znaków, ochrona danych zakończy się niepowodzeniem.

Obejście problemu: Jeśli jest konieczne przeniesienie chronionego folderu udostępnionego, należy usunąć go z grupy ochrony, a następnie dodać po przeniesieniu. W przypadku woluminu wykorzystującego szyfrowanie dopilnuj, aby nowa ścieżka pliku chronionego źródła danych była krótsza niż 5120 znaków.

Zmiana domeny zasobu chronionego

Problem: Nie można zmienić domeny komputera chronionego i kontynuować ochrony bez zakłóceń. Ponadto nie można zmienić domeny komputera chronionego i skojarzyć istniejących replik i punktów odzyskiwania z komputerem, gdy zostanie on ponownie objęty ochroną.

Obejście problemu: Odradza się zmienianie domeny komputera chronionego. Jeśli konieczna jest zmiana domeny komputera chronionego, należy najpierw usunąć ze ochrony źródła danych znajdujące się na komputerze. Następnie Włącz ochronę źródła danych na komputerze po utworzeniu nowej domeny.

Zmiana nazwy zasobu chronionego

Problem: nie można zmienić nazwy komputera chronionego i kontynuować ochrony bez zakłóceń. Ponadto nie można zmienić nazwy komputera chronionego i skojarzyć istniejących replik i punktów odzyskiwania z komputerem, gdy zostanie on ponownie objęty ochroną.

Obejście: nie zaleca się zmiany nazwy komputera chronionego. Jeśli zmiana nazwy komputera chronionego jest konieczna, najpierw wyłącz ochronę źródeł danych na tym komputerze. Następnie włącz ochronę źródła danych na tym komputerze po zmianie nazwy.

Zmiana strefy czasowej zasobu chronionego

Problem: W przypadku zmiany strefy czasowej zasobu chronionego upewnij się, że prawidłowo zaktualizowano strefę czasową.

Obejście problemu: Program DPM automatycznie rozpoznaje strefę czasową komputera chronionego podczas instalacji agenta ochrony. W przypadku przeniesienia chronionego komputera do innej strefy czasowej po skonfigurowaniu ochrony zmień strefę czasową komputera w Panelu sterowania. Następnie zaktualizuj strefę czasową w bazie danych programu DPM.

Niektóre typy danych nie są obsługiwane

Problem: Program DPM nie obsługuje następujących typów danych:

- Twarde łącza
- Punkty ponownej analizy, w tym linki systemu plików DFS i punkty połączenia.
- Metadane punktu instalacji — grupa ochrony może zawierać dane z punktami instalacji. W takim przypadku program DPM chroni zainstalowany wolumin będący elementem docelowym punktu instalacji, ale nie chroni metadanych punktu instalacji. Podczas odzyskiwania danych zawierających punkty instalacji musisz ręcznie odtworzyć hierarchię punktów instalacji.
- Dane w zainstalowanych woluminach wewnątrz zainstalowanych woluminów
- Kosz
- Pliki stronicowania
- Folder z informacjami o woluminie systemowym. Aby chronić informacje o systemie komputera, musisz

wybrać stan systemu komputera jako członka grupy ochrony.

- Woluminy z systemem plików innym niż NTFS
- Pliki zawierające twarde linki lub linki symboliczne z systemu Windows Vista.
- Pliki z dowolną spośród poniższych kombinacji atrybutów:
 - Szyfrowanie i ponowna analiza
 - Szyfrowanie i Single Instance Storage (SIS)
 - Szyfrowanie i uwzględnianie wielkości liter
 - Szyfrowanie i rozrzedzenie
 - Uwzględnianie wielkości liter i SIS
 - Kompresja i SIS

Obejście: Brak

Ograniczenia ochrony komputerów w grupach roboczych i domenach niezaufanych

Problem: Przy użyciu programu DPM można chronić obciążenia w tej samej domenie, w której znajduje się serwer DPM, lub w domenach podrzędnych i zaufanych. Można również chronić następujące obciążenia w grupach roboczych i domenach z uwierzytelnianiem przy użyciu protokołu NTLM lub certyfikatu:

- Serwer SQL
- Serwer plików
- Funkcja Hyper-V

Te obciążenia mogą działać na jednym serwerze lub w konfiguracji klastra.

Obejście problemu: Jeśli chcesz chronić obciążenia w niezaufanej domenie, zobacz [Przygotowywanie komputerów w grupach roboczych i domenach niezaufanych](#), aby zapoznać się ze szczegółowymi informacjami na temat zakresu ochrony i wymaganego rodzaju uwierzytelniania.

Krótkoterminowe kopie zapasowe na taśmie nie są obsługiwane

Problem: Program DPM nie obsługuje krótkoterminowej (przyrostowej) kopii zapasowej na taśmie dla danych obciążenia (Exchange, SQL Server, SharePoint, Hyper-V). Przyrostowe kopie zapasowe można wykonywać tylko dla danych w plikach (woluminy, udziały, foldery).

Obejście problemu: W celu utworzenia krótkoterminowej kopii zapasowej takich obciążeń użyj dysku lub dysku w połączeniu z magazynowaniem w chmurze (usługi Kopia zapasowa Azure).

Obsługa wielu długoterminowych celów kopii na taśmie, wykorzystujących zadania kopiowania zestawów danych, nie powiedzie się, jeśli zainstalowana jest tylko jedna stacja taśm

Problem: Program DPM nie obsługuje większej liczby długoterminowych celów kopii zapasowej, jeśli jest zainstalowana tylko jedna stacja taśm.

Obejście problemu: Dodaj drugą stację taśm do programu DPM lub do biblioteki taśm.

Wykonywanie kopii zapasowej danych na dyskach profilu użytkownika (UPD) nie jest obsługiwane

Problem: Przy użyciu programu DPM nie można chronić danych w udziałach plików zawierających dyski profilu użytkownika.

Obejście: brak.

Problemy związane z ochroną programu Exchange

Wykonywanie kopii zapasowej typu „z dysku na taśmę” nie jest obsługiwane w przypadku grup dostępności baz danych (DAG) programu Exchange

Problem: Program DPM nie obsługuje krótkoterminowej i długoterminowej kopii zapasowej typu „z dysku na taśmę” (D2T) w przypadku obciążeń Exchange DAG.

Obejście problemu: W przypadku obciążeń Exchange DAG użyj kopii zapasowej „z dysku na dysk i na taśmę” (D2D2T).

Problemy związane z ochroną programu SharePoint

Funkcja AlwaysOn nie jest obsługiwana

Problem: Program DPM od wersji 2012 R2 z aktualizacją 5 może chronić farmy programu SharePoint wykorzystujące bazy danych programu SQL Server z włączoną funkcją AlwaysOn.

Obejście: brak.

Problemy związane z ochroną programu SQL Server

Obsługa programu SQL Server 2014

Problem: można chronić SQL Server 2014 przy użyciu programu DPM 2012 R2 z [pakietem zbiorczym aktualizacji 4](#).

Obejście problemu: Korzystaj z właściwej wersji programu DPM.

Obsługa funkcji AlwaysOn

Problem: Funkcję AlwaysOn wprowadzono w programie SQL Server 2012. Jest ona obsługiwana przez program DPM 2012 z dodatkiem SP1 lub nowszy, zgodnie z informacjami zawartymi w temacie [Macierz obsługi ochrony programu DPM](#).

Obejście: brak.

AlwaysOn — odzyskiwanie do oryginalnej lokalizacji nie jest obsługiwane

Problem: Jeśli program DPM chroni program SQL Server z włączoną funkcją AlwaysOn, odzyskiwanie danych do oryginalnej lokalizacji nie jest obsługiwane.

Obejście: brak.

Program DPM nie może chronić programu SQL Server na serwerach plików skalowalnych w poziomie (SOFS)

Problem: Program DPM nie może chronić baz danych programu SQL Server na serwerach SOFS z systemem Windows Server 2012.

Obejście problemu: Przenieś bazy danych programu SQL Server z serwera SOFS.

Problemy związane z ochroną maszyn wirtualnych i funkcji Hyper-V

Kopia zapasowa maszyn wirtualnych z systemem Linux zawiera tylko migawki zgodne z plikami

Problem: można tworzyć kopie zapasowe maszyn wirtualnych z systemem Linux przy użyciu programu DPM 2012 R2 lub nowszego. Obsługiwane są tylko migawki zgodne z plikami.

Obejście: brak.

Wykonywanie kopii zapasowej serwerów i klastrów funkcji Hyper-V w domenach zaufanych i niezaufanych

Problem: Klastry serwerów funkcji Hyper-V muszą znajdować się w tej samej domenie, w której znajduje się serwer programu DPM, albo w domenie zaufanej lub podrzędnej, aby możliwe było wykonanie ich kopii

zapasowej. Można wykonać kopię zapasową obciążeń, serwerów i klastrów w niezaufanej domenie z uwierzytelnianiem przy użyciu protokołu NTLM lub certyfikatu dla jednego serwera albo z uwierzytelnianiem tylko przy użyciu certyfikatu dla klastra.

Obejście: Brak

Wykonywanie kopii zapasowych danych maszyny wirtualnej na dyskach przekazywania nie jest obsługiwane

Problem: Program DPM nie obsługuje wykonywania kopii zapasowych danych maszyny wirtualnej na dyskach przekazywania przekazujących woluminy do maszyny wirtualnej lub wykorzystujących zdalny plik VHD.

Obejście: W tym scenariuszu zaleca się wykonanie za pomocą programu DPM kopii zapasowej plików VHD na poziomie hosta i zainstalowanie agenta na maszynie wirtualnej w celu wykonania kopii zapasowej danych niewidocznych na gościu.

W przypadku wdrożenia skalowanego serwera DPM ochrona pomocnicza klastra funkcji Hyper-V przez program DPM nie jest obsługiwana

Problem: Jeśli klaster funkcji Hyper-V jest chroniony przez skalowany serwer DPM, nie można dodać ochrony pomocniczej chronionych obciążeń funkcji Hyper-V.

Obejście: Brak

Wykonywanie kopii zapasowej na serwerach repliki funkcji Hyper-V

Problem: Obsługa kopii zapasowej podstawowych i pomocniczych (replik) maszyn wirtualnych zależy od wersji programu DPM, zgodnie z opisem w tej tabeli.

	WINDOWS SERVER 2012 - SYSTEM OPERACYJNY HOSTA NA SERWERZE REPLIKI (POMOCNICZYM/DODATKOWYM)	WINDOWS SERVER 2012 R2 - SYSTEM OPERACYJNY HOSTA NA SERWERZE REPLIKI (POMOCNICZYM/DODATKOWYM)	WINDOWS SERVER 2012 SYSTEM OPERACYJNY HOSTA NA SERWERZE PODSTAWOWYM	WINDOWS SERVER 2012 R2 SYSTEM OPERACYJNY HOSTA NA SERWERZE PODSTAWOWYM
DPM 2012, DPM 2012 z dodatkiem SP1	Nieobsługiwane	Nieobsługiwane	Obsługiwane	Nieobsługiwane
DPM 2012 R2	Nieobsługiwane	Obsługiwane	Obsługiwane	Obsługiwane

Obejście problemu: Korzystaj z obsługiwanej wersji programu DPM, odpowiednio do danego scenariusza.

Program DPM i platforma Azure

Program DPM jako maszyna wirtualna platforma Azure

Problem: program DPM może działać jako maszyna wirtualna platformy Azure, począwszy od programu DPM 2012 R2 z aktualizacją 3. Należy pamiętać o następujących ograniczeniach:

- Lokalne serwery programu DPM nie mogą chronić obciążeń opartych na platformie Azure.
- Program DPM działający jako maszyna wirtualna IaaS na platformie Azure może chronić niektóre obciążenia działające jako maszyny wirtualne platformy Azure. Szczegółowe informacje znajdują się w temacie [DPM protection support matrix](#).
- Program DPM działający jako maszyna wirtualna platformy Azure nie może chronić obciążeń lokalnych.

Obejście problemu: Więcej informacji na temat tego scenariusza znajduje się w temacie [Install DPM as an Azure virtual machine](#).

Przygotowanie do wdrożenia serwerów programu DPM

11.12.2019 • 11 minutes to read

Przed rozpoczęciem wdrażania serwerów programu System Center Data Protection Manager (DPM) należy wziąć pod uwagę kilka czynności związanych z planowaniem:

- [Planowanie wdrożenia serwera programu DPM](#) — określ liczbę i lokalizację potrzebnych serwerów programu DPM.
- [Planowanie ustawień zapory](#) — uzyskaj informacje o ustawieniach zapory, portów i protokołów na serwerze programu DPM oraz chronionych komputerach i zdalnym serwerze programu SQL Server, jeśli jest on skonfigurowany.
- [Przyznawanie uprawnień użytkownikom](#) — określ, kto może korzystać z programu DPM.

Planowanie wdrożenia serwera programu DPM

Najpierw określ liczbę potrzebnych serwerów:

- Program DPM może chronić do 600 woluminów. Aby chronić tę maksymalną liczbę woluminów, program DPM wymaga 120 TB na jeden serwer DPM.
- Jeden serwer programu DPM może chronić maksymalnie 2000 baz danych (zalecany rozmiar dysku to 80 TB).
- Jeden serwer DPM może zabezpieczyć do 3000 komputerów klienckich i 100 serwerów.
- Do planowania pojemności serwera programu DPM można użyć [kalkulatorów pojemności magazynu programu DPM](#). Te kalkulatory są arkuszami programu Excel i ich zastosowanie zależy od obciążenia pracą. Kalkulatory dostarczają wskazówek dotyczących liczby wymaganych serwerów DPM, rdzeni procesora, pamięci RAM i pamięci wirtualnej oraz miejsca wymaganego do magazynowania. Ponieważ kalkulatory te są zależne od obciążenia, musisz traktować łącznie zalecane ustawienia i rozważyć je razem z wymaganiami systemowymi oraz topologią i wymaganiami firmy, w tym informacjami o źródłach danych i lokalizacji przechowywania, wymaganiami zgodności i umowy SLA oraz metodami odzyskiwania po awarii. Zwróć uwagę na to, że kalkulatory opracowano dla programu DPM 2010, ale działają one również z późniejszymi wersjami programu DPM.

Następnie określ lokalizację serwerów:

- Program DPM musi zostać wdrożony w domenie usługi Active Directory (system Windows Server 2008 lub nowszy).
- Podejmując decyzję o lokalizacji serwera programu DPM, uwzględnij przepustowość sieci między serwerem programu DPM i chronionymi komputerami. Jeśli chronione dane znajdują się w sieci rozległej (WAN), minimalna wymagana przepustowość sieci wynosi 512 kilobitów na sekundę (Kb/s).
- Program DPM obsługuje zespoły kart sieciowych. Zespoły kart sieciowych składają się z wielu kart fizycznych skonfigurowanych tak, aby system operacyjny traktował je jak jedną kartę. Zespoły kart sieciowych zapewniają zwiększoną przepustowość przez zsumowanie przepustowości dostępnej dla każdej karty oraz umożliwiają przełączanie w przypadku awarii karty. Program DPM może korzystać ze zwiększonej przepustowości dzięki zespołom kart skonfigurowanym na serwerze programu DPM.

- Inną ważną kwestią dotyczącą rozmieszczenia serwerów programu DPM jest konieczność ręcznego zarządzania taśmami i bibliotekami taśm, na przykład podczas dodawania nowych taśm do biblioteki lub przenoszenia ich do archiwum poza siedzibą firmy.
- Serwer programu DPM może chronić zasoby w jednej domenie lub w różnych domenach w obrębie lasu, który ma ustanowioną dwukierunkową relację zaufania z domeną, w której znajduje się serwer programu DPM. Jeśli między domenami nie istnieje dwukierunkowa relacja zaufania, musisz skonfigurować oddzielny serwer programu DPM dla każdej domeny. Serwer programu DPM może chronić dane znajdujące się w różnych lasach, jeśli między tymi lasami istnieje dwukierunkowe zaufanie.
- Należy rozważyć przepustowość sieci między serwerem DPM i komputerami chronionymi. Jeśli chronione dane znajdują się w sieci WAN, wymagana minimalna przepustowość sieci to 512 Kb/s. Należy pamiętać, że program DPM obsługuje zespoły kart sieciowych, co zwiększa przepustowości dzięki połączeniu przepustowości dostępnej dla poszczególnych kart oraz zapewnia tryb failover w przypadku awarii.

Planowanie ustawień zapory i uprawnień użytkowników

Ustawienia zapory

Skonfigurowanie ustawień zapory pod kątem wdrożenia programu DPM jest wymagane na serwerze programu DPM, na komputerach, które mają być chronione, oraz na serwerze programu SQL Server używanym do komunikacji z bazą danych programu DPM w przypadku zdalnego korzystania z tej bazy. Jeśli podczas instalacji programu DPM jest włączona Zapora systemu Windows, to ustawienia zapory zostaną automatycznie skonfigurowane na serwerze programu DPM. Ustawienia zapory podsumowano w poniższej tabeli.

LOKALIZACJA	REGUŁA	SZCZEGÓŁY	PROTOKÓŁ	PORT
Serwer programu DPM	Ustawienia modelu DCOM programu System Center Data Protection Manager	Używane na potrzeby komunikacji DCOM między serwerem programu DPM a chronionymi komputerami.	DCOM	135/TCP (dynamiczny)
Serwer programu DPM	System Center Data Protection Manager	Wyjątek dla programu Msdpmp.exe (usługi programu DPM). Uruchamiany na serwerze programu DPM.	Wszystkie protokoły	Wszystkie porty
Serwer programu DPM Chronione komputery	Agent replikacji programu System Center Data Protection Management	Wyjątek dla programu Dpmra.exe (usługi agenta ochrony używanej do tworzenia kopii zapasowej i przywracania danych). Uruchamiany na serwerze programu DPM i chronionych komputerach.	Wszystkie protokoły	Wszystkie porty
Chronione komputery		Konfigurowanie przychodzącego wyjątku dla programu sqserv.exe		

LOKALIZACJA	REGUŁA	SZCZEGÓŁY	PROTOKÓŁ	PORT
Chronione komputery		Program DPM wydaje polecenia agentowi ochrony za pomocą wywołań DCOM wysyłanych do agenta. Aby umożliwić komunikację programowi DPM, należy otworzyć górne porty (1024–65535).	DCOM	135/TCP (dynamiczny)
Chronione komputery		Kanał danych programu DPM korzysta z protokołu TCP. Zarówno serwer programu DPM, jak i chronione komputery inicjują połączenia. Program DPM komunikuje się z koordynatorem agenta przez port 5718, a z agentem ochrony przez port 5719.	TCP	5718/TCP 5719/TCP
Chronione komputery		Używane do rozpoznawania nazw hostów między programem DPM/chronionym komputerem a kontrolerem domeny.	systemem DNS,	53/UDP
Chronione komputery		Używane do uwierzytelniania punktu końcowego połączenia między programem DPM/chronionym komputerem a kontrolerem domeny.	Kerberos	88/UDP 88/TCP
Chronione komputery		Używane do przesyłania zapytań między serwerem programu DPM a kontrolerem domeny.	LDAP	389/TCP 389/UDP

LOKALIZACJA	REGUŁA	SZCZEGÓŁY	PROTOKÓŁ	PORT
Chronione komputery		Używane do wykonywania różnych operacji między 1) programem DPM a chronionymi komputerami; 2) programem DPM a kontrolerem domeny; 3) chronionymi komputerami a kontrolerem domeny. Używane również dla ruchu SMB obsługiwanego bezpośrednio przez protokół TCP/IP na potrzeby funkcji programu DPM.	NetBIOS	137/UDP 138/UDP 139/TCP 445/TCP
Zdalny serwer programu SQL Server		Włączenie protokołu TCP/IP dla wystąpienia DPM programu SQL Server z następującymi funkcjami: domyślna inspekcja niepowodzeń, włączenie sprawdzania zasad haseł.		
Zdalny serwer programu SQL Server		Włączenie wyjątku ruchu przychodzącego dla programu sqservr.exe dla wystąpienia DPM programu SQL Server w celu umożliwienia ruchu TCP przez port 80. Serwer raportów nasłuchuje żądań HTTP na porcie 80.		
Zdalny serwer programu SQL Server		Domyślne wystąpienie aparatu bazy danych nasłuchuje żądań TCP na porcie 1443. Ustawienie to może być modyfikowane. Aby usługa SQL Server Browser mogła łączyć się przez port inny niż domyślny, należy ustawić port UDP 1434.		

LOKALIZACJA	REGUŁA	SZCZEGÓŁY	PROTOKÓŁ	PORT
Zdalny serwer programu SQL Server		Nazwane wystąpienie programu SQL Server domyślnie używa portów dynamicznych. Ustawienie to może być modyfikowane.		
Zdalny serwer programu SQL Server		Włączenie usługi RPC		

Udzielanie uprawnień użytkownika

Przed rozpoczęciem wdrażania programu DPM sprawdź, czy odpowiednim użytkownikom przyznano uprawnienia wymagane do wykonywania różnych zadań. Podsumowanie dotyczące tych raportów można znaleźć w poniższej tabeli.

ZADANIE PROGRAMU DPM	WYMAGANE UPRAWNIENIA
Dodawanie serwera programu DPM do domeny	Konto administratora domeny lub uprawnienie użytkownika umożliwiające dodawanie stacji roboczej do domeny
Instalowanie programu DPM	Konto administratora na serwerze programu DPM
Instalowanie agenta ochrony programu DPM na komputerze, który ma być chroniony	Konto domeny, które należy do lokalnej grupy administratorów na komputerze
Rozszerzanie schematu usługi AD w celu włączenia odzyskiwania przez użytkownika końcowego	Uprawnienia administratora schematu w domenie
Tworzenie kontenera usługi AD w celu włączenia odzyskiwania przez użytkownika końcowego	Uprawnienia administratora domeny
Przyznawanie serwerowi programu DPM uprawnień do zmiany zawartości kontenera	Uprawnienia administratora domeny
Włączanie odzyskiwania przez użytkownika końcowego na serwerze programu DPM	Konto administratora na serwerze programu DPM
Instalowanie oprogramowania klienckiego punktu odzyskiwania na komputerze chronionym	Konto administratora na komputerze
Uzyskiwanie dostępu do poprzednich wersji chronionych danych z poziomu komputera chronionego	Konto użytkownika z dostępem do udziału chronionego
Odzyskiwanie danych programu SharePoint	Administrator farmy programu SharePoint będący jednocześnie administratorem serwera frontonu sieci Web, na którym zainstalowano agenta ochrony.

Przygotowywanie środowiska dla programu System Center Data Protection Manager

09.03.2020 • 18 minutes to read

Podczas wdrażania programu System Center — Data Protection Manager (DPM) 2016 lub nowszego, Użyj poniższych informacji do zaplanowania środowiska.

Zagadnienia dotyczące wdrażania programu DPM

Jedną z pierwszych decyzji jest sposób wdrożenia programu DPM. Program DPM można wdrożyć:

- **Jako fizyczny serwer autonomiczny** — możesz wdrożyć program DPM jako fizyczny serwer autonomiczny służący do wykonywania kopii zapasowych danych lokalnych. Serwerów fizycznych programu DPM nie można wdrożyć w klastrze, ale można zarządzać wieloma serwerami fizycznymi z poziomu pojedynczej konsoli, instalując centralną konsolę na System Center Operations Manager.
- **Jako maszynę wirtualną funkcji Hyper-v** — program DPM można uruchomić jako maszynę wirtualną (hostowaną na lokalnym serwerze hosta funkcji Hyper-v), aby utworzyć kopię zapasową danych lokalnych. Listę zagadnień związanych z tym środowiskiem można znaleźć w artykule Instalowanie programu DPM jako maszyny wirtualnej na lokalnym serwerze funkcji Hyper-V.
- **Jako maszynę wirtualną z systemem Windows w oprogramowaniu VMware** — można wdrożyć program DPM w celu zapewnienia ochrony obciążeń firmy Microsoft działających na maszynach wirtualnych z systemem Windows w oprogramowaniu VMware. W tym scenariuszu program DPM można wdrażać jako autonomiczny serwer fizyczny, jako maszynę wirtualną funkcji Hyper-V lub jako maszynę wirtualną systemu Windows w środowisku VMWare.
- **Jako maszynę wirtualną platformy Azure** — program DPM może działać jako maszyna wirtualna na platformie Azure w celu tworzenia kopii zapasowych obciążeń chmury działających jako maszyny wirtualne platformy Azure. Informacje dotyczące tego wdrożenia można znaleźć w artykule Instalowanie programu DPM jako maszyny wirtualnej platformy Azure.

We wszystkich wdrożeniach, które będą potrzebne:

- Wystąpienie SQL Server zainstalowane i uruchomione, które ma być używane dla DPM database. Wystąpienie może być umieszczone na serwerze DPM lub na serwerze zdalnym.
- Dysk używany wyłącznie do przechowywania danych programu DPM.
- Agent ochrony programu DPM zainstalowany na komputerach i serwerach, które chcesz chronić za pomocą oprogramowania DPM.

Baza danych programu SQL Server

Serwer DPM wykorzystuje program SQL Server jako bazę danych służącą do przechowywania informacji o kopii zapasowej dla obciążeń, serwerów i komputerów, które chroni. Wszystkie SQL Server wersje powinny mieć wersję Standard lub Enterprise 64-bit.

NOTE

- W przypadku obsługiwanych wersji programu SQL należy używać tych pakietów, które są obecnie obsługiwane przez firmę Microsoft.
- W przypadku poniższych obsługiwanych wersji SQL, standard, Enterprise i Datacenter (64-bitowe) są obsługiwane w zależności od dostępności.

Obsługiwane wersje SQL Server

WERSJA PROGRAMU DPM	WERSJA SQL
DPM 2016	SQL Server 2014 SP2; SQL Server 2012 SP4.
Program DPM 2016 UR2 i nowsze	SQL Server 2016 i SPs w sposób szczegółowy
DPM 1801	SQL Server 2016 i SPs w sposób szczegółowy
DPM 1807 i DPM 2019	-SQL Server 2016 i SPs w sposób szczegółowy -SQL Server 2017 zgodnie z opisem w tym miejscu

Wymagania dotyczące programu SQL Server

WYMAGANIE	SZCZEGÓŁY
Pamięć RAM	Minimalna 4 GB, zalecane 8 GB
Dysk	Minimalna 1 GB, zalecane 3 GB
Wymagane funkcje	Usługi aparatu bazy danych, usługi Reporting Services (dla programu DPM 2019, Instalowanie usług SSRS przy użyciu programu SQL 2017) Uwaga — W przypadku zdalnego serwera SQL, aparatu bazy danych i usług raportowania musi znajdować się na tym samym komputerze. . — W przypadku zdalnego klastrowanego wystąpienia SQL aparat bazy danych musi znajdować się w klastrze, a SSRS musi znajdować się na osobnym komputerze, który może być serwerem DPM lub innym komputerem)
Sortowanie	SQL_Latin1_General_CP1_CI_AS
Porty dynamiczne	Obsługiwane
AlwaysOn	Nieobsługiwane
Instalacja	Zainstaluj program SQL Server na serwerze zdalnym lub na serwerze DPM. Program SQL Server należy zainstalować i uruchomić przed instalacją serwera DPM.

WYMAGANIE	SZCZEGÓŁY
Instalacja zdalna	Zainstaluj w tej samej domenie i strefie czasowej co serwer DPM. Gdy jest używany do obsługi programu DPM, SQL Server nie może udostępnić serwera z kontrolerem domeny. Przeczytaj Konfigurowanie zdalnego wystąpienia programu SQL Server. Jeśli wdrażasz program DPM jako maszynę wirtualną platformy Azure, możesz określić maszynę wirtualną platformy Azure z uruchomioną SQL Server jako wystąpienie SQL Server zdalnego. Nie można używać na lokalnym serwerze SQL. Używanie bazy danych SQL Azure nie jest obecnie obsługiwane.
Program SQL Server w klastrze	Obsługiwane

NOTE

Jeśli uaktualniasz SQL Database do programu SQL 2017, upewnij się, że zainstalowano uaktualnianie SQL usługi SQL SSRS.

Serwer DPM

WYMAGANIE	SZCZEGÓŁY
System operacyjny	System Windows Server 2019, Datacenter i wersje Standard (system Windows Server Core 2019 jest obsługiwany w programie DPM 2019 UR1) Windows Server 2016, Datacenter i wersje Standard Windows Server 2012 R2, Datacenter i wersje Standard (nie dotyczy programu DPM 2019)
Wymagania wstępne instalacji	Microsoft .NET Framework 4,5 lub nowszy (dla 2019) Microsoft .NET Framework 4.0 Instalator Windows 4.5 lub nowsze wersje Windows PowerShell 3.0 Magazyn SIS systemu Windows Raportowanie błędów aplikacji firmy Microsoft Narzędzia do zarządzania SQL (dla programu DPM 2019) Instalator automatycznie instaluje wymagania wstępne, jeśli nie zostały jeszcze zainstalowane.
Ograniczenia	Program DPM można zainstalować na woluminie systemu operacyjnego lub na innym woluminie. Program DPM jest przeznaczony do działania na dedykowanym, wyznaczonym do tego celu serwerze. Nie należy instalować programu DPM na: — serwerze pełniącym rolę serwera aplikacji, — serwerze zarządzania programem Operations Manager, — serwerze programu Exchange, — serwerze działającym w węźle klastra. Program DPM nie jest obsługiwany w tureckich wersjach językowych wszystkich obsługiwanych wersji systemu Windows Server.

Dyski i magazyn

WYMAGANIE	MINIMALNIE	ZALECANE
Dysk	Wymagania programu DPM: — Dysk służący do instalacji programu DPM zawierający system plików, pliki instalacyjne, wstępnie wymagane oprogramowanie i pliki bazy danych — Dysk przeznaczony dla puli magazynów	
Instalacja programu DPM	Lokalizacja instalacji programu DPM: 3 GB Dysk na pliki bazy danych: 900 MB Dysk systemowy: 1 GB Obszar na dysku przeznaczony na dysk systemowy jest wymagany, jeśli na serwerze DPM jest zainstalowany serwer SQL. W przypadku zdalnego serwera SQL wystarczy znacznie mniej wolnego miejsca przeznaczonego na dysk systemowy.	Każdy chroniony wolumin wymaga co najmniej 300 MB wolnego miejsca na dziennik zmian. Ponadto podczas archiwizowania należy skopiować katalog plików do tymczasowej lokalizacji instalacji programu DPM. dla woluminu instalacyjnego programu DPM zalecana jest 2-3 GB wolnego miejsca.
Dysk puli magazynów	1,5 raza więcej niż rozmiar chronionych danych	2–3 razy więcej niż rozmiar chronionych danych
Numer jednostki logicznej (LUN) <i>Dotyczy tylko serwerów programu DPM 2016/2019 uaktualnionych z programu DPM 2012 R2, które używają starszej puli magazynów.</i>		Maksymalnie 17 TB dla dysków dynamicznych z tabelą partycji GUID (GPT) 2 TB dla dysków z głównym rekordem rozruchowym (MBR) Wymagania są oparte na maksymalnym rozmiarze dysku twardego, który jest widoczny w systemie operacyjnym.
Ograniczenia <i>Dotyczy tylko serwerów DPM 2016/DPM 2019 uaktualnionych z programu DPM 2012 R2, które używały starszej puli magazynów.</i>	-Pule magazynów programu DPM muszą być dynamiczne. — Nie można zainstalować programu DPM na dysku używanym dla puli magazynów. — Można dołączyć lub skojarzyć niestandardowe woluminy z chronionymi źródłami danych. Woluminy niestandardowe mogą znajdować się na dyskach podstawowych lub dynamicznych, ale nie jest możliwe zarządzanie miejscem na tych woluminach za pomocą konsoli administratora programu DPM. — Można utworzyć kopię zapasową na taśmie przy użyciu biblioteki taśm dołączonych do iSCSI. Firma Microsoft zaleca stosowanie osobnej karty dla takiego połączenia. Aby uzyskać dodatkowe informacje, zobacz zgodne biblioteki taśm .	

WYMAGANIE	MINIMALNIE	ZALECANE
Zwirtualizowany program DPM	— Program DPM działający na maszynie wirtualnej może używać następujących typów magazynu: — Dysk VHD spełniający wymagania dotyczące konfiguracji wymienione w temacie opisującym instalowanie programu DPM w środowisku wirtualnym — Dysk przekazujący z bezpośrednio dołączonym magazynem (DAS) hosta — Przekazująca jednostka LUN iSCSI dołączona do hosta — Przekazująca jednostka LUN Fibre Channel dołączona do hosta — Docelowa jednostka LUN iSCSI podłączona bezpośrednio do maszyny wirtualnej programu DPM — Jednostka LUN Fibre Channel podłączona do maszyny wirtualnej programu DPM przy użyciu kontrolera Windows Server 2012 Virtual Fiber Channel (VFC)	
Modern Backup Storage	Używa woluminów podstawowych, nie może znajdować się na dysku dynamicznym. Pojedynczy serwer programu DPM ma limit niezmienny dla magazynu 120 TB.	

Zalecenia dotyczące magazynu dla programu DPM

- Rozmiar sektora powinien zawsze być spójny w ramach podstawowego magazynu (tj. WS Storage) do magazynu natywnego programu DPM.
- Gdy funkcja miejsca do magazynowania jest używana do wydzielenie magazynu programu DPM, funkcja miejsca do magazynowania jest obsługiwana na kontrolerach iSCSI i FC, o ile nie są one odporne na błędy (proste z dowolną liczbą kolumn)
- Pamięć podręczna zapisu powinna zawsze wynosić od SE do zero przy użyciu funkcji miejsca do magazynowania dla magazynu programu DPM.

Chronione obciążenia robocze

WYMAGANIE	SZCZEGÓŁY
Limity rozmiaru chronionego obciążenia	Program DPM 2016 i nowszy z Nowoczesny magazyn kopii zapasowych nie mają limitów LDM. W przypadku programu DPM 2016 i nowszych można chronić więcej danych na serwerze DPM. Przetestowano maksymalnie 120 TB limitu magazynowania na serwer DPM. Jednak 120 TB jest tylko ograniczeniem elastycznym. Sprawdzanie poprawności jest w toku w celu przetestowania wyższego limitu. Te wskazówki zostaną zaktualizowane po zakończeniu walidacji.

WYMAGANIE	SZCZEGÓŁY
.NET Framework	Przed instalacją agenta ochrony DPM na wszystkich chronionych komputerach musi być zainstalowany program .NET Framework w wersji 4.0 lub wyższej.
Windows Management Framework (WMF) (Nie dotyczy programu DPM 2019)	W przypadku ochrony serwera wydanego przed systemem Windows Server 2012 należy zainstalować odpowiednią wersję programu WMF przed zainstalowaniem agenta DPM: - WMF 3.0 dla systemu Windows Server 2008 z dodatkiem SP2 - WMF 4.0 dla systemów Windows 7, Windows Embedded Standard 7 i Windows Server 2008 R2 Systemy Windows Server 2012 i nowsze nie wymagają oddzielnej instalacji programu WMF.
Chronione obciążenia robocze	W dokumencie Macierz obsługi ochrony programu DPM znajduje się aktualna lista obciążeń chronionych.
Wymagania wstępne	Na chronionym komputerze musi być zainstalowany agent ochrony programu DPM. Aby uzyskać więcej informacji, zobacz Konfigurowanie agenta ochrony. Woluminy chronione nie mogą być mniejsze niż 1 GB i muszą mieć format NTFS. Systemy operacyjne serwerów chronionych przez program DPM muszą być 64-bitowe.

Obsługa sieci

WYMAGANIE	SZCZEGÓŁY
Domena	Serwer DPM powinien znajdować się w systemie Windows Server 2019, Windows Server 2016, Windows Server 2012 R2, Windows Server 2012
Zaufanie domeny	Program DPM obsługuje funkcje ochrony danych w wielu lasach, o ile zostanie nawiązana dwukierunkowa relacja zaufania między oddzielnymi lasami. Program DPM może chronić serwery i stacje robocze w domenach w lesie, który ma ustanowioną dwukierunkową relację zaufania z domeną serwera DPM. Bez dwukierunkowej relacji zaufania program DPM nie może chronić komputerów w grupach roboczych lub domenach niezaufanych. Aby uzyskać więcej informacji, zobacz Tworzenie kopii zapasowych i przywracanie obciążeń w grupach roboczych i domenach niezaufanych.
Konfiguracja sieci	W przypadku ochrony danych przy użyciu sieci rozległej (WAN) minimalna przepustowość sieci musi wynosić 512 kilobitów na sekundę (kb/s). Program DPM nie obsługuje rozłączonych obszarów nazw.

Zdalne zarządzanie

WYMAGANIE	SZCZEGÓŁY
Program Central Console	Użyj konsoli centralnej do administrowania wieloma serwerami DPM z jednej lokalizacji. Zainstaluj ją na serwerze z programem System Center 2016/2019 Operations Manager. Należy także zainstalować agenta programu Operations Management na serwerze DPM. Zobacz Instalowanie konsoli centralnej.
Powłoka zarządzania programem DPM	Zainstaluj powłokę zarządzania serwera DPM na komputerze klienckim, aby bezpośrednio zarządzać co najmniej jednym serwerem DPM za pomocą programu Windows PowerShell. Zainstaluj ją, używając instalatora programu DPM. Powłokę zarządzania programem DPM można zainstalować na komputerach z systemem: DPM 2019: Windows Server 2019, Windows Server 2016, Windows 8.1 i Windows 10 DPM 2016: Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Windows 7, Windows 8, Windows 8.1 Uwaga: program DPM 2019 obsługuje tylko komputery 64-bitowe.
Konsola administracji zdalnej	Skonfiguruj konsolę administracji zdalnej w celu zarządzania pojedynczym serwerem DPM. Powłokę zarządzania programem DPM można zainstalować na komputerach z systemem Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Windows 7, Windows 8, Windows 8.1 i Windows 10. Na komputerze musi być uruchomione środowisko .NET Framework w wersji 4.0 lub nowszej. Uwaga: program DPM 2019 obsługuje tylko komputery 64-bitowe.

Przygotowanie magazynu danych

11.12.2019 • 31 minutes to read

Główna część wdrożenia programu System Center Data Protection Manager (DPM) będzie dowiedzieć się, jak przechowywać dane kopii zapasowej wykonywanej przez program DPM. Dowiedz się więcej:

- [Dodawanie magazynu za pomocą funkcji Modern Backup Storage](#)
- [Przechowywanie krótkoterminowe i długoterminowe](#)
- [Przechowywanie w chmurze przy użyciu usługi Azure Backup](#)
- [Przechowywanie na dysku](#)
- [Przechowywanie na taśmie](#)

Krótkoterminowe i długoterminowe Omówienie magazynu

W programie DPM należy wybrać krótkie i długoterminowe przechowywanie kopii zapasowych danych.

MAGAZYN	KRÓTKOTERMINOWE	DŁUGOTERMINOWE	CECHY
Chmura Azure	Odpowiednie dla przechowywania krótkoterminowego	Odpowiednie dla przechowywania długoterminowego	— Efektywne i ekonomiczne rozwiązanie w zakresie krótkoterminowego i długoterminowego przechowywania poza siedzibą firmy. — Platforma Azure może być używana jako magazyn dla danych funkcji Hyper-V, programu SQL Server i serwera plików. Platformy Azure można używać tylko do tworzenia kopii zapasowych danych z serwerów z systemem Windows Server 2016, Windows Server 2012 R2, Windows Server 2012 lub Windows Server 2008 R2 z dodatkiem SP1. — Aby korzystać z usługi Azure Backup, należy uruchomić program DPM w ramach rozwiązania System Center 2012 z dodatkiem SP1 lub nowszym.
Taśma	W przypadku niektórych obciążeń roboczych kopie zapasowe można zapisywać bezpośrednio na taśmie (D2T) na potrzeby przechowywania krótkoterminowego. Dotyczy to danych	W przypadku wszystkich obciążeń roboczych kopie zapasowe można zapisywać na taśmie w celu długoterminowego przechowywania poza firmą (D2D2T).	— Krótkoterminowe kopie zapasowe na taśmie mogą być przydatne dla danych, które nie zmieniają się często, przez co nie wymagają częstego wykonywania kopii zapasowych. -Długoterminowy magazyn

MAGAZYN	KRÓTKOTERMINOWE plikowych (woluminy, działy, foldery), stanu systemu, programu SQL Server, funkcji Hyper-V i baz danych Exchange, które nie są skonfigurowane dla grupy DAG.	DŁUGOTERMINOWE	CECHY taśm poza siedzibą firmy jest przydatny w przypadku danych, które muszą być przechowywane w celu spełnienia obowiązkowych zobowiązań — Jeśli taśmy są używane do ochrony długoterminowej i krótkoterminowej, program DPM tworzy kopie najnowszych krótkoterminowych pełnych kopii zapasowych i używa ich do generowania długoterminowych kopii zapasowych na taśmach. Zaleca się zaplanowanie uruchamiania wykonywania krótkoterminowej kopii zapasowej dzień przed wykonaniem długoterminowej kopii zapasowej. W ten sposób można zapewnić, że do wykonania długoterminowej kopii zapasowej będzie używana najnowsza krótkoterminowa kopia zapasowa. — Jeśli używasz dysku do krótkoterminowej kopii zapasowej i taśmy do celów długoterminowych, długoterminowe kopie zapasowe będą pobierane z repliki dysku. — Odzyskiwanie danych z taśmy może być powolne, dlatego jest lepszym rozwiązaniem w przypadku danych z wysokim wskaźnikiem celu punktu odzyskiwania (RPO), które nie muszą być dostępne i odzyskiwane w krótkim okresie krytycznym po awarii. — Nie można zwolnić miejsca na taśmie ani wymazać taśmy zawierającej poprawne punkty odzyskiwania. Należy usunąć źródła z grupy ochrony i spowodować wygaśnięcie punktów odzyskiwania lub zmodyfikować ustawienia grupy ochrony w celu wyłączenia ochrony taśmy. Aby wygaśnić taśmę, oznacz ją jako wolną, a następnie usuń jej oznaczenie i ponownie zavykazuj. — Wykonywanie kopii zapasowych na taśm i

MAGAZYN	KRÓTKOTERMINOWE	DŁUGOTERMINOWE	zapasowych na taśmie i odzyskiwanie może wymagać prac manualnych, na przykład przy rotacji taśm. — Pojemność pamięci masowej na długoterminowe kopie zapasowe można zwiększyć przez dodanie taśm. — Biblioteka taśm lub autonomiczna stacja taśm musi być fizycznie podłączona do serwera programu DPM. Biblioteka taśm może być podłączona bezpośrednio interfejsem SCSI lub za pośrednictwem sieci SAN.
Dysk	Wszystkie kopie zapasowe danych w programie DPM można krótkoterminowo przechowywać na dysku (D2D).	Nie można tworzyć długoterminowych magazynów na dyskach.	— Dyski umożliwiają szybkie tworzenie kopii zapasowych i odzyskiwanie danych. Jest to rozwiązanie przydatne w przypadku danych o małym celu punktu odzyskiwania (RPO), czyli wymagających szybkiego odzyskania po awarii. — Nadmiarowość dysków można uzyskać za pomocą technologii, takich jak macierze RAID. — Maksymalny czas przechowywania danych na dysku to 448 dni. — Wykonywanie kopii zapasowej na dysku nie ma wpływu na działające zadania.

Przygotowanie magazynu w chmurze (Azure Backup)

Usługa Azure Backup umożliwia zapisywanie kopii zapasowych danych chronionych przez program DPM na platformie Azure. Jest to przydatne w kilku przypadkach:

- **Program DPM wdrożony lokalnie jako serwer fizyczny lub na maszynie wirtualnej** — w przypadku wdrożenia programu DPM jako serwera fizycznego lub lokalnej maszyny wirtualnej funkcji Hyper-V można utworzyć kopię zapasową danych przy użyciu usługi Azure Backup (jako dodatek do tworzenia kopii zapasowej danych na dysku i taśmie).
- **Program DPM wdrożony jako maszyna wirtualna na platformie Azure** — jeśli program DPM jest wdrożony na maszynie wirtualnej platformy Azure (możliwe od programu System Center 2012 R2 z aktualizacją Update 3), możesz utworzyć kopię zapasową danych na dyskach platformy Azure dołączonych do maszyny wirtualnej programu DPM na platformie Azure, a następnie odciążyć magazyn danych, tworząc kopię zapasową w usłudze Azure Backup.

Podczas konfigurowania grupy ochrony w programie DPM należy wybrać opcję dysk do krótkoterminowego przechowywania, a następnie włączyć tworzenie kopii zapasowych online na platformie Azure. Należy pamiętać o następujących kwestiach:

- Obowiązuje kilka wymagań wstępnych i ograniczeń. [Przeczytaj więcej](#).
- Aby można było włączyć opcję kopii zapasowych w chmurze dla grupy ochrony w konsoli programu DPM, należy najpierw skonfigurować usługę Azure Backup. [Dowiedz się](#), jak skonfigurować usługę Azure Backup przy użyciu programu DPM.

Przygotowanie magazynu dyskowego

Program DPM zapisuje kopie danych na dysku w celu przechowywania krótkoterminowego, zapisując dane w puli magazynów. Pula magazynów to zestaw dysków i woluminów, na których serwer DPM przechowuje punkty odzyskiwania chronionych danych. Aby można było przechowywać dane na dysku, musisz mieć co najmniej jeden dysk lub wolumin w puli magazynów. W przypadku puli magazynów można użyć dowolnego z poniższych rozwiązań:

NOTE

Nie zaleca się używania serwera NAS jako magazynu w celu przygotowania magazynu dyskowego programu DPM.

- Bezpośrednio dołączony magazyn (DAS)
- Sieć magazynowania (SAN) Fiber Channel
- Urządzenie magazynujące iSCSI lub sieć SAN

Najlepsze rozwiązania w zakresie puli magazynów

NAJLEPSZE ROZWIĄZANIE	SZCZEGÓŁY
-----------------------	-----------

NAJLEPSZE ROZWIĄZANIE	SZCZEGÓŁY
Ograniczenia dysków	— Serwer programu DPM musi mieć zainstalowane co najmniej dwa dyski. Dedykowany dysk rozruchowy, zawierający system i pliki instalacyjne programu DPM, oraz drugi dysk przeznaczony dla puli magazynów. W programie DPM dysk jest zdefiniowany jako dowolne urządzenie dyskowe jako dysk w narzędziu Zarządzanie dyskami systemu Windows. Do puli magazynów nie można dodać dysków zawierających pliki rozruchowe lub systemowe albo dowolny składnik instalacji programu DPM. — Dyski dodane do puli magazynów nie powinny mieć partycji. Aby przygotować dyski, program DPM ponownie sformatuje dyski i wymazuje wszelkie dane. -Pula magazynów obsługuje większość typów dysków, w tym IDE, SATA i SCSI, a pula magazynów obsługuje zarówno główny rekord rozruchowy (MBR), jak i tabelę partycji GUID (GPT). Firma Microsoft zdecydowanie zaleca korzystanie z dysków GPT. — Jeśli dla puli magazynów jest używana sieć SAN, firma Microsoft zaleca utworzenie oddzielnej strefy dla dysku i taśmy. Nie mieszaj urządzeń w jednej strefie. — Program DPM nie obsługuje dysków USB/1394 w puli magazynów. — Nie można używać funkcji miejsca do magazynowania dla puli magazynów dyskowych. — Niektórzy producenci oryginalnego sprzętu (OEM) zawierają partycję diagnostyczną zainstalowaną z nośnika, który zapewnia. Partycja diagnostyczna może być również nazywana partycją OEM lub partycją EISA. Partycje EISA należy usunąć z dysków przed dodaniem ich do puli magazynów. — Woluminy niestandardowe zdefiniowane w konsoli Zarządzanie dyskami można zamienić na woluminy w puli magazynów. -Zalecamy używanie rozszerzalnego sprzętu, aby można było dodać więcej pojemności, jeśli jest to konieczne.
Obsługa deduplikacji	Program DPM działający jako maszyna wirtualna Hyper-V może przechowywać dane kopii zapasowych w plikach VHD w folderach udostępnionych na serwerze plików z systemem Windows z włączoną deduplikacją. Więcej informacji znajduje się w temacie Deduplikacja magazynu programu DPM.

NAJLEPSZE ROZWIĄZANIE	SZCZEGÓŁY
Wymagania dotyczące pojemności	Wymagania dotyczące pojemności są zależne przede wszystkim od rozmiaru chronionych danych, codziennego rozmiaru punktu odzyskiwania, oczekiwanego tempa rozrostu danych woluminu oraz od docelowego zakresu przechowywania. Codzienny rozmiar punktu odzyskiwania to łączny rozmiar zmian wprowadzonych do chronionych danych w ciągu jednego dnia. Jest w przybliżeniu równy rozmiarowi przyrostowej kopii zapasowej. Zakres przechowywania to liczba dni, przez jaką punkty odzyskiwania danych chronionych mają być przechowywane na dysku. W przypadku plików program DPM może przechowywać maksymalnie 64 punkty odzyskiwania dla każdego woluminu z grupy chronionej. Dla każdej grupy ochrony może codziennie utworzyć maksymalnie 8 zaplanowanych w harmonogramie punktów odzyskiwania. Zakres przechowywania to liczba dni, przez jaką punkty odzyskiwania danych chronionych mają być przechowywane na dysku. W przypadku plików program DPM może przechowywać maksymalnie 64 punkty odzyskiwania dla każdego woluminu z grupy chronionej. Dla każdej grupy ochrony może codziennie utworzyć maksymalnie 8 zaplanowanych w harmonogramie punktów odzyskiwania. Limit 64 punktów odzyskiwania dla plików wynika z ograniczenia usługi kopiowania woluminów w tle (VSS). Ograniczenie liczby punktów odzyskiwania nie obowiązuje w przypadku danych aplikacji. Zalecamy utworzenie puli magazynów dwukrotnie większej niż rozmiar chronionych danych. Wynika to z zakładanego codziennego rozmiaru punktu odzyskiwania na poziomie 10% rozmiaru chronionych danych oraz zakresu przechowywania równego 10 dni. Aby prawidłowo oszacować rozmiar, można sprawdzić przyrostową kopię zapasową dla typowego dnia. Jeśli na przykład przyrostowa kopia zapasowa 100 GB danych ma rozmiar 10 GB, oznacza to, że codzienny rozmiar punktu odzyskiwania będzie wynosić około 10 GB. Oczywiście należy dostosować założenie 10% i 10 dni dla szacowania zgodnie z wymaganiami organizacji. Im większy zakres przechowywania, tym mniej punktów odzyskiwania można utworzyć każdego dnia. Jeśli na przykład zakres przechowywania jest równy 64 dni, każdego dnia można utworzyć tylko jeden punkt odzyskiwania. Jeśli jest to 8 dni, każdy dzień można utworzyć 8 punktów odzyskiwania. Przy zakresie przechowywania wynoszącym 10 dni każdego dnia można utworzyć około 6 punktów odzyskiwania.

NAJLEPSZE ROZWIĄZANIE	SZCZEGÓŁY
Konfiguracja dyskowa	W przypadku używania bezpośrednio dołączonego magazynu z pulą magazynów można zastosować dowolną sprzętową konfigurację macierzy RAID albo konfigurację grupy dysków (JBOD). W przypadku dysków, które mają być dodane do puli magazynów, nie należy tworzyć programowej konfiguracji RAID. Decydując o konfiguracji dysków, należy uwzględnić specyficzne dla używanego środowiska priorytety dotyczące pojemności, kosztów, niezawodności oraz wydajności. Jeśli na przykład w konfiguracji JBOD przestrzeń dyskowa potrzebna na dane parzystości jest niewielka, można ją zastosować w celu uzyskania możliwie największej ilości miejsca do magazynowania. Jednak niezawodność konfiguracji JBOD jest mała. Awaria jednego dysku powoduje natychmiastową utratę danych. W typowym wdrożeniu programu DPM jest zalecana konfiguracja RAID 5, która zapewnia efektywny kompromis między pojemnością, kosztem, niezawodnością i wydajnością. Aby ułatwić ocenę opcji dotyczących konfigurowania dysków dla puli magazynów, poniższa tabela zawiera porównanie wad i zalet konfiguracji JBOD oraz różnych poziomów macierzy RAID w skali od 4 (bardzo dobre) do 1 (akceptowalne).
Wartości niestandardowe	W niektórych przypadkach może być konieczne użycie woluminu niestandardowego, który nie należy do puli magazynów i jest używany do przechowywania repliki oraz punktów odzyskiwania dla członka grupy ochrony. Na przykład może być wymagana większa kontrola nad magazynem dla konkretnych źródeł danych lub dane krytyczne muszą być przechowywane przy użyciu jednostki LUN o wysokiej wydajności w sieci SAN. Jako wolumin niestandardowy można wybrać dowolny wolumin dołączony do serwera programu DPM z wyjątkiem woluminu, który zawiera pliki systemowe i pliki programów. Aby użyć woluminów niestandardowych jako elementów członkowskich grupy ochrony, muszą być dostępne dwa woluminy niestandardowe: jeden wolumin do przechowywania repliki i jeden wolumin do przechowywania punktów odzyskiwania. Program DPM nie może zarządzać przestrzenią woluminów niestandardowych. Jeśli program DPM ostrzega, że na woluminie niestandardowym z repliką lub woluminie z punktem odzyskiwania kończy się wolne miejsce, należy ręcznie zmienić rozmiar woluminu niestandardowego za pomocą konsoli Zarządzanie dyskami. Po utworzeniu grupy nie można zmienić puli magazynów ani woluminu niestandardowego wybranych dla członka grupy ochrony. Aby to zrobić, zatrzymaj ochronę źródła danych, a następnie dodaj je ponownie do grupy zabezpieczeń.

Porównanie opcji dysków

Dysk

KONFIGURACJA DYSKOWA	POJEMNOŚĆ	KOSZT	NIEZAWODNOŚĆ	WYDAJNOŚĆ/SKALOW ALNOŚĆ
JBOD	4	4	1	4
RAID 0	4	4	1	4
RAID 1	1	1	4	3
RAID 5	3	3	3	3
RAID 10	1	1	4	4

Konfigurowanie puli magazynów

Po skonfigurowaniu co najmniej jednego dysku zgodnie z warunkami wstępnymi można dodać go do puli magazynów.

- W konsoli administratora programu DPM kliknij pozycje **Zarządzanie > Dyski**.
- Kliknij przycisk **Dodaj** na Wstążce narzędzi i w oknie **Dodaj dyski do puli magazynów** wybierz dysk do dodania z listy **dostępne dyski**.

Po skonfigurowaniu puli magazynów podczas tworzenia grup ochrony zawierających źródła danych, dla których chcesz utworzyć kopię zapasową, będzie można skonfigurować dysk jako krótkoterminowy magazyn dla tej kopii zapasowej danych.

Przygotowywanie kopii zapasowej na taśmie

- Program DPM może tworzyć kopie zapasowe bibliotek taśm lub autonomicznych stacji taśm.
- Należy dodać biblioteki taśm lub autonomiczną stację taśm do serwera programu DPM przy użyciu sieci SAN lub interfejsu SCSI. Stacje taśm muszą być zgodne z programem DPM. Zapoznaj się z tematem [Określanie zgodnych bibliotek taśm](#).
- Uzyskaj listę [zgodnych bibliotek taśm](#).
- Wymagana pojemność taśm jest zależna od rozmiaru chronionych danych i liczby zadań tworzenia kopii zapasowej na taśmach, które muszą zostać uruchomione. Aby zaplanować liczbę taśm wymaganych dla danej grupy ochrony, należy pomnożyć wymaganą częstotliwość tworzenia kopii zapasowych przez zakres przechowywania.
- W przypadku autonomicznych stacji taśm program DPM wykonuje dla każdej grupy ochrony następujące operacje:
 - Dołącza wszystkie krótkoterminowe kopie zapasowe do pojedynczej taśmy.
 - Dołącza wszystkie długoterminowe kopie zapasowe do pojedynczej taśmy, która jest inna od taśmy z krótkoterminowymi kopiami zapasowymi.
 - Gdy taśma się zapełni, program DPM generuje alert informujący o konieczności dodania nowej wolnej taśmy.
- Dla bibliotek taśm:
 - Program DPM może przydzielić dwie taśmy (lub większą ich liczbę) do każdej grupy ochrony. Wszystkie źródła danych w grupie ochrony są zawsze dołączane do tej samej taśmy niezależnie od wybranego rodzaju ochrony — krótkoterminowej lub długoterminowej.

- Jeśli ustawienia grupy ochrony określają przydział więcej niż jednej stacji, źródła danych zostaną podzielone na poszczególnej taśmie. Jeśli na przykład istnieje pięć źródeł danych, a stacja ma ustawiony limit dwóch źródeł, program DPM może zapisać trzy źródła danych na jednej taśmie i dwa na innej. Może to spowodować nierównomierny rozkład danych między taśmami, w zależności od rozmiaru danych, innych zadań zaplanowanych kopii zapasowych i liczby stacji taśm dostępnych w tym czasie.
- Długoterminowe kopie zapasowe na taśmach przydzielają daną taśmę do każdego zadania tworzenia pełnej kopii zapasowej, co sprawia, że wszystkie punkty odzyskiwania długoterminowych kopii zapasowych zawsze znajdują się na nowej taśmie.
- Liczba dostępnych wolnych taśm zmniejsza się wraz z przydzielaniem taśm do długoterminowych lub krótkoterminowych kopii zapasowych. Jeśli nie jest dostępna nowa taśma do długoterminowej kopii zapasowej, zostanie wygenerowany alert.
- Jeśli krótkoterminowe kopie zapasowe są skonfigurowane do korzystania z taśm i jest używana opcja tworzenia pełnej kopii zapasowej, wszystkie zadania tworzenia pełnej kopii zapasowej będą wymagały nowej wolnej taśmy.
- Jeśli użytkownik zainicjuje dwie różne akcje „utwórz punkt odzyskiwania (taśma)” dla dwóch członków grupy ochrony, program DPM utworzy dwa zadania tworzenia kopii zapasowej na taśmach, co sprawi, że będą wymagane dwie taśmy. Jeśli użytkownik zainicjuje jedną akcję „utwórz punkt odzyskiwania (taśma)” dla dwóch członków grupy ochrony, zostanie użyta jedna taśma. W ten sposób w przypadku kopii zapasowych ad hoc dane wybranych członków grupy ochrony są zawsze umieszczane na tej samej taśmie.

Instalowanie i konfigurowanie urządzeń taśmowych

1. Dołączyć stację taśm — wykonaj instrukcje dostarczone z urządzeniem taśmowym w celu podłączenia i zainstalowania go na serwerze programu DPM.
2. Sprawdzić numery seryjne — sprawdź, czy zmieniające nośników i stacje taśm mają numery seryjne. DPM używa ich do identyfikacji. Zainstalowane urządzenia taśmowe znajdują się na liście w Menedżerze urządzeń.
3. Dodać wyjątki zapory — dodaj wyjątki zapory, aby program DPM mógł wykryć taśmę:


```
C:\Program Files\Microsoft System Center
2012\DPM\SQL\SSQL10_50.MSDPMV4RC\MSSQL\Binn\sqlservr.exe C:\Program Files
(x86)\Microsoft SQL Server\90\Shared\sqlbrowser.exe C:\Program Files\Microsoft System Center
2012\DPM\DPM\bin\DPMLA.exe
```
4. Dodać wyjątki zapory — dodaj wyjątki zapory, aby program DPM mógł wykryć taśmę:


```
C:\Program Files\Microsoft System Center
2012\DPM\SQL\SSQL10_50.MSDPMV4RC\MSSQL\Binn\sqlservr.exe C:\Program Files
(x86)\Microsoft SQL Server\90\Shared\sqlbrowser.exe C:\Program Files\Microsoft System Center
2012\DPM\DPM\bin\DPMLA.exe
```
5. Wykryć ręcznie — serwer programu DPM automatycznie wykrywa urządzenia taśmowe podłączone do niego fizycznie. Są one wyświetlane w obszarze roboczym Biblioteki w widoku Zarządzanie. Jeśli urządzenie nie jest wyświetlane, można wykryć je ręcznie przy użyciu przycisku Skanuj ponownie. Może to potrwać kilka minut. Po ponownym skanowaniu sprawdź, czy szczegółowe dane wyświetlane w Menedżerze urządzeń i w bibliotece taśm są identyczne.
6. Konfigurowanie udostępniania taśm — skonfiguruj udostępnianie taśm, jeśli chcesz udostępnić jedną bibliotekę taśm na wielu serwerach programu DPM. Należy pamiętać o następujących kwestiach:
 - Biblioteka taśm to zwykle zestaw stacji taśm, które automatycznie instalują i odinstalowują nośniki taśmowe.

- Biblioteka taśm musi się działać w środowisku sieci SAN.

7. Serwer biblioteki to komputer, na którym jest zainstalowany program DPM, wykonane zostało polecenie udostępnienia biblioteki i jest włączony zmieniacz nośników. Klient biblioteki to komputer, na którym jest zainstalowany program DPM, wykonane zostało polecenie udostępnienia biblioteki i nie jest włączony zmieniacz nośników. Zalecane jest, by konfiguracja systemowa komputera serwera biblioteki i wszystkich komputerów klientów biblioteki była jak najbardziej podobna. Nie zaleca się konfigurowania żadnych grup ochrony na serwerze biblioteki.
8. Wszystkie serwery programu DPM używające udostępnionej biblioteki muszą używać podobnej konfiguracji programu SQL Server do obsługi baz danych programu DPM. Na przykład wszystkie powinny używać wystąpienia lokalnego bazy danych programu DPM albo wszystkie powinny używać wystąpienia zdalnego. Nie może być tak, że niektóre serwery programu DPM używają wystąpienia lokalnego, a inne wystąpienia zdalnego.

Po skonfigurowaniu taśm podczas tworzenia grupy ochrony zawierającej źródła chronionych danych można wybrać taśmę do długoterminowego i krótkoterminowego przechowywania danych.

Jeśli chcesz użyć biblioteki udostępnionej dla wielu serwerów programu DPM, kontynuuj od następnej procedury.

Konfigurowanie udostępniania taśm

1. Na komputerze, który będzie serwerem biblioteki dla biblioteki udostępnionej, użyj Menedżer urządzeń, aby włączyć zmieniacz nośników.

Na każdym komputerze klienta biblioteki zmieniacz nośników musi być wyłączony.

2. Włącz protokół nazwanych potoków dla wystąpień programu SQL Server na komputerach serwera biblioteki i klientów biblioteki. Następnie uruchom ponownie usługę SQL.
3. Aby skonfigurować serwery programu DPM do użycia biblioteki udostępnionej, na każdym komputerze klienta biblioteki otwórz okno Wiersz polecenia z podwyższonym poziomem uprawnień, a następnie uruchom następujące polecenia:

- `cd <system drive>:\Program Files\Microsoft System Center 2012 R2\DPM\DPM\Setup`
- `AddLibraryServerForDpm.exe -DpmServerWithLibrary <FQDN of library server>`, gdzie "<nazwa FQDN serwera biblioteki>" to w pełni kwalifikowana nazwa domeny serwera biblioteki.

4. Na komputerze serwera biblioteki otwórz okno Wiersz polecenia z podwyższonym poziomem uprawnień, a następnie uruchom następujące polecenia jeden raz dla każdego klienta biblioteki. Na przykład jeśli serwer biblioteki obsługuje trzech klientów biblioteki, polecenie trzeba uruchomić na serwerze biblioteki trzy razy.

- `cd <system drive>:\Program Files\Microsoft System Center 2012 R2\DPM\DPM\Setup`
- `AddLibraryServerForDpm.exe - ShareLibraryWithDpm <FQDN of library client>`, gdzie `<FQDN of library client>` to w pełni kwalifikowana nazwa domeny klienta biblioteki.

5. Przed uruchomieniem poniższych poleceń na wszystkich komputerach klienckich biblioteki upewnij się, że usługi SQL Server (MSDPM2012) i SQL Server Agent (MSDPM2012) używają konta użytkownika domeny jako konta logowania. Upewnij się również, że konto domeny jest członkiem lokalnej grupy administratorów na wszystkich komputerach, które współużytkują bibliotekę. Następnie na każdym komputerze klienta biblioteki Otwórz okno Wiersz polecenia z podwyższonym poziomem uprawnień i uruchom następujące polecenia.

- `cd <system drive>:\Program Files\Microsoft System Center 2012 R2\DPM\DPM\Setup`
- `SetSharedDpmDatabase -DatabaseName <SqlServer\Instance\DatabaseName> [-DoNotMoveData]`, gdzie

<SQLServer\Instance\Databasename> jest nazwą bazy danych serwera biblioteki. Nazwę można znaleźć w oknie **Informacje o programie DPM** w konsoli administratora programu DPM.

6. W Konsola administratora programu DPM na serwerze biblioteki wykonaj ponowne skanowanie. Następnie wykonaj ponowne skanowanie lub odświeżenie na każdym komputerze klienckim biblioteki.

Najszybszym sposobem na wyświetlenie wszystkich nośników na wszystkich serwerach DPM jest wykonanie na każdym z nich ponownego skanowania, a następnie szczegółowego spisu. Następnie na jednym z serwerów należy oznaczyć wybrane nośniki jako wolne, po czym wykonać odświeżenie na pozostałych serwerach. Po skonfigurowaniu udostępniania biblioteki można używać udostępnionej biblioteki taśm, tak jak gdyby była dołączona do każdego serwera programu DPM.

Następne kroki

Po zaplanowaniu magazynu należy zapoznać się z artykułem [Identyfikowanie zgodnych bibliotek taśm](#).

Jeśli chcesz zainstalować program DPM, zapoznaj się z artykułem [Instalowanie programu DPM](#).

Określanie zgodnych bibliotek taśm

10.01.2020 • 7 minutes to read

Użyj witryny TechNet wiki, aby znaleźć najnowszą listę [zgodnych bibliotek taśm](#) dla programu System Center Data Protection Manager (DPM).

Obsługa wirtualnej biblioteki taśm

Wirtualne biblioteki taśm skonfigurowane za pomocą wirtualnej karty Fibre Channel są obsługiwane z certyfikowanym sprzętem wymienionym w witrynie typu wiki. Aby sprawdzić, czy dana biblioteka taśm jest obsługiwana przez wirtualną kartę Fibre Channel, poproś dostawcę sprzętu taśm o sprawdzenie zgodności biblioteki taśm.

Sprawdzanie zgodności biblioteki taśm

Jeśli taśma znajduje się w [katalogu systemu Windows Server](#) w sekcji sprzętu i magazynowania, a także została oznaczona jako zgodna z 64-bitowym systemem Windows 2008 lub 64-bitowym systemem Windows 2008 R2, będzie ona prawdopodobnie współdziałać z programem DPM. Należy pamiętać, że wszelkimi niezgodnościami w zakresie sterowników w systemie Windows 2012 musi zająć się dostawca. Jeśli masz już taśmę, możesz uruchomić narzędzie Test zgodności biblioteki taśm programu DPM.

Uruchamianie narzędzia sprawdzania zgodności

Przed uruchomieniem narzędzia wykonaj następujące czynności:

- Upewnij się, że docelowa biblioteka taśm oraz stacje taśm są widoczne w Menedżerze urządzeń.
- Włóż taśmę danych przeznaczoną do odczytu i zapisu do gniazda 0. Zawartość tej taśmy zostanie zastąpiona.
- Włóż taśmę czyszczącą do gniazda 1. Taśmy muszą znajdować się w kolejnych gniazdach, a w gniazdach między tymi taśmami nie mogą znajdować się inne taśmy. Gniazdo z taśmą z danymi musi poprzedzać gniazdo z taśmą czyszczącą.

Aby uzyskać i uruchomić narzędzie sprawdzania zgodności:

1. Pobierz [narzędzie Test zgodności biblioteki taśm programu DPM](#).
2. Wyodrębnij pliki. Otwórz wiersz polecenia z podwyższonym poziomem uprawnień, a następnie przejdź do folderu, do którego wyodrębniono narzędzie.
3. Aby sprawdzić, czy narzędzie wykrywa taśmę, wpisz polecenie **DPMLibraryTest.exe /CERTIFY /LL**. Przeprowadź certyfikację w następujący sposób:
 - Aby przeprowadzić certyfikację biblioteki taśm, wpisz polecenie
`DPMLibraryTest.exe /CERTIFY /TL <tape library name> /AT`
 - Aby przeprowadzić certyfikację autonomicznej stacji taśm, wpisz polecenie
`DPMLibraryTest.exe /CERTIFY /TL <device name> /SA`
4. Narzędzie uruchomi następujące testy:
 - **Test 1: konfiguracja podstawowa** — ten test polega na skanowaniu systemu pod kątem dołączonych urządzeń oraz identyfikowaniu autonomicznych stacji taśm i bibliotek taśm. Po

zakończeniu testu narzędzie wyświetli podsumowanie. Dla każdego urządzenia zostaną wyświetlone następujące właściwości: nazwa urządzenia, numer seryjny, nazwa dostawcy, nazwa produktu, wersja oprogramowania układowego i właściwości interfejsu SCSI. Należy sprawdzić, czy informacje w posumowaniu są prawidłowe. Jeśli nie są:

- Sprawdź, czy w Menedżerze urządzeń są wyświetlone wszystkie urządzenia.
- Upewnij się, że sterowniki urządzeń są aktualne.
- Jeśli mapowania dysków są nieprawidłowe, należy użyć narzędzia DPMDriveMapping.exe <w folderze instalacji programu DPM>folderze/bin., aby poprawić mapowania. Jeżeli na komputerze nie zainstalowano programu DPM, skopiuj plik DPMLA.xml utworzony przez narzędzie DPMDriveMapping.exe do folderu zawierającego wyodrębnione narzędzie certyfikacji biblioteki taśm.

- **Test 2: instalowanie/odinstalowywanie** — ten test wybiera taśmę z pierwszego dostępnego gniazda, a następnie instaluje taśmę w stacji i odinstalowuje ją z niej.
- **Test 3: czyszczenie stacji** — przeprowadza test czyszczenia za pomocą taśmy czyszczącej. W przypadku korzystania z programu Firestreamer w ramach biblioteki VTL nie można usuwać ani zmieniać taśm. Aby pominąć ten test, użyj w składni flagi /ST.
- **Test 4: nośnik I/E** — ten test wybiera pierwszą dostępną taśmę i przenosi ją do portu I/E i z powrotem. Jeżeli biblioteka/VTL nie zawiera portów I/E, narzędzie automatycznie pominie ten test.
- **Test 5: we/wy** — ten test wybiera pierwszą zapisywalną taśmę, zapisuje na niej kilka buforów, a następnie próbuje odczytać zapisane dane. Ten test służy tylko do sprawdzenia możliwości odczytu/zapisu. Konkretnie błędy na dysku należy sprawdzić za pomocą trybu zaawansowanego.

5. Gdy narzędzie ukończy test, informacje dziennika zostaną zapisane w plikach LibraryTestTool-*Curr.errlog znajdujących się w folderze, z poziomu którego narzędzie zostało uruchomione. Jeśli testy zostaną zakończone pomyślnie, można założyć, że biblioteka taśm będzie współdziałać z programem DPM.

Uruchamianie narzędzia sprawdzania zgodności dla funkcji Hyper-V protokołu Fibre Channel

- Przygotuj dwa hosty funkcji Hyper-V z uruchomionym programem DPM.
- Włącz migrację na żywo na obydwu serwerach. Klastrowane wdrożenie nie jest wymagane.
- Uruchom narzędzie zgodności na pierwszym serwerze hosta zgodnie z opisem w powyższej sekcji i sprawdź, czy testy zakończyły się pomyślnie.
- Zainicjuj migrację na żywo na drugim serwerze hosta, a następnie zaczekaj na jej zakończenie.
- Jeśli program DPM działa wirtualnie na drugim serwerze hosta, uruchom narzędzie sprawdzania zgodności na tym serwerze hosta zgodnie z opisem w powyższej sekcji, a następnie sprawdź, czy testy zostały pomyślnie zakończone. Jeśli tak, można założyć, że biblioteka taśm będzie współdziałać z programem DPM.

Przykłady

Składnia narzędzia jest następująca:

```
DPMLibraryTest.exe /CERTIFY /<switch_1> [/switch_2]
```

PRZEŁĄCZNIK	DETAILS	PRZYKŁAD
/LL	Wyświetlanie dostępnych bibliotek i stacji taśm	DPMLibraryTest.exe /CERTIFY /LL
/LT	Wyświetlanie wszystkich przypadków testowych	
/TL	Test biblioteki	
/AT	Uruchamianie wszystkich testów	Uruchamianie testu w bibliotece fizycznej: DPMLibraryTest.exe /CERTIFY /TL \\\\.\\Changer0 /AT
/ST	Uruchamianie określonych testów	Uruchamianie tylko testów 3 i 4 w bibliotece fizycznej. DPMLibraryTest.exe /CERTIFY /TL \\\\.\\Changer0 /ST 3 4 Uruchamianie wszystkich testów oprócz testu czyszczenia: DPMLibraryTest.exe /CERTIFY /TL \\\\.\\Changer0 /ST 1 2 4 5
/SA	Uruchamianie testów stacji autonomicznej	DPMLibraryTest.exe /CERTIFY /TL \\\\.\\Tape21745678 /SA
/EX	Wyświetlanie przykładów	
/Help lub /?	Wyświetlanie pomocy	

Określanie źródeł danych, które mają być chronione

11.12.2019 • 2 minutes to read

Aby chronić źródła danych za pomocą programu System Center Data Protection Manager (DPM), należy wykonać następujące czynności:

- Przeczytaj artykuł [What can DPM back up?](#) (Co program DPM może umieścić w kopii zapasowej?), aby dowiedzieć się, dla jakich plików można tworzyć kopie zapasowe w programie DPM.
- Program DPM stosuje ustawienia dotyczące kopii zapasowych do wszystkich źródeł danych w danej grupie ochrony. Należy ustalić sposób umieszczenia danych w grupach, które mają być chronione. Przykłady obejmują:
 - **Według komputera** — wszystkie źródła danych komputera należą do tej samej grupy ochrony. Dzięki temu można w jednym miejscu zmieniać ustawienia wpływające na obciążenie zasobów komputera. Jednak wszystkie źródła danych będą mieć te same ustawienia wykonywania kopii zapasowych i przywracania.
 - **Według obciążenia** — pliki i typy danych poszczególnych aplikacji będą przydzielone do różnych grup ochrony. Umożliwia zarządzanie zadaniami jako grupami. Jednak odzyskanie serwera z wieloma aplikacjami może wymagać wielu taśm z różnych grup ochrony.
 - **Według celu punktu/czasu odzyskiwania** — zebranie razem źródeł danych o podobnych celach punktu odzyskiwania (Recovery Point Objective, RPO) i celach czasu odzyskiwania (Recovery Time Objective, RTO). Docelowy punkt odzyskania można kontrolować przez ustawienie dla grupy ochrony częstotliwości synchronizacji, która wpływa na ilość danych (mierzoną czasem), które mogą zostać utracone w przypadku awarii. Docelowy czas odzyskania to dopuszczalna długość czasu, przez który dane będą niedostępne. Zależy on od metod przechowywania kopii zapasowych wybranych dla grupy ochrony.
 - **Według cech danych** — na przykład częstotliwość zmian danych, szybkość ich przyrostu lub ich wymagania dotyczące pamięci masowej.

Następne kroki

[Wdrażanie agenta ochrony programu DPM](#)

Get DPM installed (Instalowanie programu DPM)

06.03.2020 • 33 minutes to read

Oto co należy zrobić, aby skonfigurować program System Center Data Protection Manager (DPM):

1. Przeczytaj [Wymagania wstępne instalacji](#)
2. Sprawdź, czy [system operacyjny programu DPM](#) jest zgodny.
3. [Skonfiguruj bazę danych programu SQL Server](#) do przechowywania ustawień i danych konfiguracji programu DPM.
4. Skonfiguruj program DPM. Możesz [zainstalować program DPM](#) z poziomu interfejsu użytkownika lub [uruchomić instalację nienadzorowaną](#). Wykonaj te instrukcje, aby [zainstalować program DPM na kontrolerze domeny](#)

Wymagania wstępne instalacji

ŚRODOWISKO	SZCZEGÓŁY INSTALACJI
Podstawowe wymagania wstępne instalacji programu DPM	Serwer DPM musi zawierać kilka składników. Te z nich są instalowane automatycznie podczas instalacji: —.NET Framework 4,0 lub 4,5 (DPM 2016/2019); .NET Framework 3,5 wymagane do instalacji bazy danych SQL (przed SQL 2016); .NET Framework 4,6 wymagany do instalacji bazy danych SQL (SQL 2016 lub nowsza). Jeśli nie zostanie zainstalowana automatycznie, zainstaluj ją za pomocą opcji dodawania funkcji w Menedżerze serwera. — Instalator Windows 4.5 (lub nowszy). Instalowany w ramach systemu operacyjnego, ale można go również zainstalować jako administrator z DPM\setup\redist\WindowsInstaller\INSTMSI45. EXE. — Pakiet redystrybucyjny programu Microsoft Visual C++ 2012; pakiet redystrybucyjny programu Microsoft Visual C++ 2010; pakiet redystrybucyjny programu Microsoft Visual C++ 2008. — Program PowerShell 3,0 (dołączony do systemu Windows Server 2012 R2 lub 2012)

ŚRODOWISKO	SZCZEGÓŁY INSTALACJI
DPM database	- sprawdzić obsługiwane wersje SQL Server dla DPM Database. — SQL Server można zainstalować na serwerze DPM lub na serwerze zdalnym. — W przypadku zdalnej instalacji bazy danych maszyna, na której jest uruchomione zdalne wystąpienie, musi znajdować się w tej samej domenie i strefie czasowej co serwer DPM. — Jeśli używasz zdalnej bazy danych, przygotuj ją przed zainstalowaniem programu DPM. — Nie można uruchomić SQL Server na kontrolerze domeny. — Jeśli używasz zdalnej bazy danych, przygotuj ją przed zainstalowaniem programu DPM. Upewnij się, że narzędzie przygotowania bazy danych SQL na zdalnym komputerze SQL Server zostało uruchomione. — Program SQL Server może być autonomiczny lub może działać w klastrze. — Nie można użyć SQL Server zawsze włączone wdrożenie. — W przypadku wdrożenia programu DPM jako maszyny wirtualnej platformy Azure należy użyć maszyny wirtualnej platformy Azure z SQL Server jako wystąpienia SQL Server zdalnego. Nie można używać SQL Server lokalnych w tym wdrożeniu, a korzystanie z Azure SQL Database nie jest obecnie obsługiwane. — Jeśli SQL Server jest klastrowane, serwer raportowania i SQL Server powinny znajdować się na różnych komputerach.

ŚRODOWISKO	SZCZEGÓŁY INSTALACJI
Program DPM instalowany jako maszyna wirtualna funkcji Hyper-V	W przypadku instalacji programu DPM jako maszyny wirtualnej funkcji Hyper-V należy pamiętać o następujących kwestiach: • Wirtualna instalacja programu DPM nie jest przeznaczona dla środowisk skalowalnych. Zamiast tego należy korzystać z magazynu dołączanego bezpośrednio lub opartego na sieci SAN. W razie korzystania z plików VHDX w środowiskach skalowalnych (funkcja Hyper-V na udostępnionym woluminie klastra) wydajność może być gorsza niż w przypadku sieci SAN. Z tego względu nie zaleca się używania plików VHDX w środowiskach skalowalnych. • Pliki VHDX nie mają limitu rozmiaru. Są obsługiwane zarówno pliki VHDX o stałym rozmiarze jak i dynamicznie powiększające się. • Pula magazynów programu DPM obsługuje zarówno pliki VHD, jak i VHDX. Wirtualna instalacja programu DPM jest wymagana w celu umożliwienia obsługi dodawania wirtualnych dysków twardych do puli magazynów. • W przypadku dynamicznych wirtualnych dysków twardych i wirtualnych dysków twardych o stałym rozmiarze pliki VHD i VHDX są obsługiwane w zdalnych udziałach SMB. • Od wersji DPM 2012 R2 z pakietem Update 3 można uruchamiać program DPM jako maszynę wirtualną funkcji Hyper-V z obsługą stacji taśm za pomocą syntetycznego protokołu Fibre Channel. • W przypadku magazynu programu DPM o wysokiej dostępności wirtualne dyski twarde powinny być umieszczane na skalowalnych w poziomie serwerach plików (SOFs). Skalowalne w poziomie serwery plików wymagają protokołu SMB 3.0. • Wirtualne instalacje programu DPM nie obsługują: ◦ miejsc do magazynowania systemu Windows 2012 ani wirtualnych dysków twardych zainstalowanych w miejscach do magazynowania; lokalnego lub zdalnego hostingu plików VHDX w miejscach do magazynowania systemu Windows 2012; ◦ włączonej deduplikacji dysku na woluminach zawierających wirtualne dyski twarde; ◦ obiektów docelowych iSCSI systemu Windows 2012 (korzystających z wirtualnych dysków twardych) jako puli magazynów programu DPM; ◦ kompresji NTFS woluminów zawierających pliki VHD używane w puli magazynów programu DPM; ◦ Funkcja BitLocker w woluminach zawierających pliki VHD używane w puli magazynów. ◦ plików VHDX w puli magazynów programu DPM na dyskach fizycznych, których sektory mają macierzysty rozmiar 4 KB; ◦ wirtualnych dysków twardych udostępnianych na serwerach systemu Windows 2008.

• Program DPM jest obsługiwany na maszynie wirtualnej modelu IaaS platformy Azure o rozmiarze A2 lub większym.

Aby wybrać rozmiar maszyny wirtualnej programu DPM, możesz skorzystać z [kalkulatora rozmiaru maszyny wirtualnej platformy Azure programu DPM](#). Po skonfigurowaniu maszyny wirtualnej utwórz wystąpienie w standardowej warstwie obliczeniowej, ponieważ maksymalna liczba operacji wejścia/wyjścia na sekundę na dysku dołączonym jest większa w warstwie standardowej niż w warstwie podstawowej.

- Program DPM może chronić obciążenia, tak jak to opisano w artykule [Matrix Protection](#).

- Program DPM może chronić obciążenia uruchamiane w ramach wielu usług w chmurze platformy Azure, które korzystają z tej samej sieci wirtualnej platformy Azure i subskrypcji platformy Azure.

W programie DPM uruchomionym jako maszyna wirtualna platformy Azure nie można chronić danych lokalnych.

- Należy użyć oddzielnego konta magazynu dla maszyny wirtualnej programu DPM, ponieważ jego rozmiar i limity liczby operacji wejścia/wyjścia na sekundę mogą mieć wpływ na wydajność maszyny wirtualnej programu DPM, jeśli konto jest udostępniane innym uruchomionym maszynom wirtualnym. Maszyna wirtualna programu DPM i chronione obciążenia powinny być częścią tej samej sieci wirtualnej platformy Azure.

- Liczba dysków, które mogą być używane w magazynie docelowym (puli magazynów programu DPM), jest ograniczona przez rozmiar maszyny wirtualnej (maksymalnie 16). Agent usługi Azure Backup działający na serwerze programu DPM wymaga tymczasowego magazynu do własnego użytku (lokalizacja pamięci podręcznej) oraz dla danych przywróconych z chmury (lokalny obszar przemieszczania). Należy zwrócić uwagę, że każda maszyna wirtualna platformy Azure ma tymczasowy magazyn danych na dysku. Jest on dostępny dla użytkownika jako wolumin D:\. Lokalny obszar przemieszczania wymagany dla usługi Azure Backup można skonfigurować na dysku D:\, a lokalizację pamięci podręcznej można umieścić na dysku C:\. Dzięki temu nie trzeba używać miejsca na dyskach danych dołączonych do maszyny wirtualnej programu DPM.

- Dane są przechowywane na dyskach platformy Azure dołączonych do maszyny wirtualnej programu DPM. Po dołączeniu do maszyny wirtualnej dyski i ilość miejsca do magazynowania będą zarządzane w programie DPM. Ilość danych, dla których można utworzyć kopię zapasową, zależy od liczby i rozmiaru dysków dołączonych do maszyny wirtualnej programu DPM. Istnieje maksymalna liczba dysków, które można dołączyć do każdej maszyny wirtualnej platformy Azure (4 dyski dla A2V2, A4V2, A8V2) i maksymalny rozmiar każdego dysku (1 TB). Na podstawie tych danych określana jest całkowita dostępna pojemność puli magazynów kopii zapasowych. Firma Microsoft zaleca zachowywanie danych przez jeden dzień na dysku platformy Azure z dołączonym programem DPM i przechowywanie danych starszych niż jeden dzień w usłudze Azure

ŚRODOWISKO	Backup. Zapewnia to dłuższy zakres przechowywania magazynu danych i umożliwia ochronę większej ilości danych dzięki przeniesieniu ich do usługi Kopia zapasowa Azure. SZCZEGÓŁY INSTALACJI - Możesz korzystać z następujących opcji skalowania wdrożenia: - Opcja 1, skalowanie w górę: zwiększanie rozmiaru maszyny wirtualnej programu DPM z A2V2, A4V2, A8V2 i Dodawanie więcej magazynu lokalnego. - Opcja 2, odciążanie od danych: wysyłanie starszych danych do usługi Kopia zapasowa Azure i zachowywanie tylko najnowszych danych w magazynie dołączonym do serwera programu DPM. - Opcja 3, skalowanie w poziomie: dodawanie kolejnych serwerów programu DPM w celu włączenia ochrony obciążeń. - Poniższa Tabela A zawiera podsumowanie maksymalnej liczby chronionych obciążeń dla każdego rozmiaru maszyny wirtualnej programu DPM.
-------------------	--

Tabela A

ROZMIAR MASZYN WIRTUALNEJ	MAKSYMALNA LICZBA CHRONIONYCH OBCIĄŻEŃ	ŚREDNI ROZMIAR OBCIĄŻENIA	ŚREDNIA WARTOŚĆ ZMIAN OBCIĄŻENIA (DZIENNE)
A2V2	20	100 GB	5% zmian netto
A4V2	40	150 GB	10% zmian netto
A8V2	60	200 GB	15% zmian netto

Konfigurowanie bazy danych programu SQL Server

Skonfigurowanie bazy danych programu SQL Server jest konieczne w następujących przypadkach:

- Korzystasz z programu DPM 2019, 2016

Aby skonfigurować bazę danych programu SQL Server:

- Uruchom instalatora programu SQL Server na serwerze lokalnym, na którym zainstalujesz program DPM, bądź na serwerze zdalnym.
- Na karcie **Instalacja** kliknij opcję **Nowy serwer SQL instalacji autonomicznej** lub **dodaj funkcje do istniejącej instalacji**.
- Na karcie **Klucz produktu** wprowadź ważny klucz licencji. Na karcie **Reguły obsługi instalacji** napraw wszystkie błędy przed kontynuowaniem instalacji. Na karcie **Rola instalatora** wybierz opcję **Instalacja funkcji programu SQL Server**
- Na karcie **Wybór funkcji** wybierz opcję **Usługi aparatu bazy danych**. W polu **Funkcje wystąpienia** wybierz opcję **Usługi raportowania — w trybie macierzystym**. Na karcie **Zasady instalacji** zapoznaj się z zasadami.
- Na karcie **Konfiguracja wystąpienia** podaj nazwę wystąpienia programu SQL Server, którego chcesz użyć na potrzeby programu DPM. W nazwie nie używaj znaku podkreślenia ani znaków zlokalizowanych.

Na karcie **Wymagania dotyczące miejsca na dysku** zapoznaj się z wymaganiami.

6. Na karcie **Konfiguracja serwera** -> **Konta usług** podaj konta domen, przy użyciu których mają być uruchamiane usługi programu SQL Server:

- Zaleca się, aby do uruchamiania usług programu SQL Server, agenta programu SQL Server, aparatu bazy danych programu SQL Server i usług SQL Server Reporting Services używać jednego, przeznaczonego tylko do tego celu konta użytkownika domeny.
- W przypadku instalowania programu DPM na kontrolerze RODC należy użyć utworzonego tam konta DPMSQLSvcsAcct. Należy pamiętać, że konto użytkownika musi być członkiem lokalnej grupy administratorów na kontrolerze domeny, na którym jest zainstalowane wystąpienie zdalne. Po zakończeniu instalacji można usunąć konto użytkownika z lokalnej grupy administratorów. Ponadto na potrzeby instalacji na kontrolerze RODC będzie trzeba wprowadzić hasło wybrane podczas konfigurowania kontrolera RODC dla programu DPM i tworzenia konta DPMR\$MACHINE_NAME.
- Podczas tworzenia konta użytkownika domeny nadaj mu najmniejsze możliwe uprawnienia, przypisz silne hasło, które nie wygaśnie, i nadaj mu łatwą do rozpoznania nazwę. To konto należy później dodać w kreatorze do lokalnej grupy administratorów i do stałej roli serwera Sysadmin programu SQL Server.
- Wszystkim usługom, z wyjątkiem uruchamiania demona filtra pełnotekstowego SQL, należy nadać wartość Automatyczny.

7. Na karcie **Konfiguracja aparatu bazy danych** zaakceptuj ustawienie Tryb uwierzytelniania systemu Windows. Administratorzy programu DPM potrzebują uprawnień *administratora SQL Server*. W obszarze **określ SQL Server Administratorzy** Dodaj administratorów programu DPM. W razie potrzeby możesz dodać dodatkowe konta. Wykonaj pozostałe kroki kreatora, używając ustawień domyślnych, i kliknij polecenie **Gotowy do zainstalowania** -> **Instaluj**.

8. W przypadku instalacji programu SQL Server na komputerze zdalnym należy wykonać następujące czynności:

- Zainstaluj pliki obsługi programu DPM (SQLPrep). W tym celu na komputerze z programem SQL Server włóż dysk DVD programu DPM i uruchom plik setup.exe. Użyj kreatora, aby zainstalować pakiet redystrybucyjny programu Microsoft Visual C++ 2012. Pliki obsługi programu DPM zostaną zainstalowane automatycznie.
- Skonfiguruj reguły zapory tak, aby serwer DPM mógł komunikować się z komputerem programu SQL Server:
 - Upewnij się, że protokół TCP/IP jest włączony z ustawieniami **domyślna inspekcja niepowodzeń i włączone sprawdzanie zasad haseł**.
 - Aby umożliwić ruch TCP na porcie 80, skonfiguruj wyjątek ruchu przychodzącego dla pliku sqservr.exe dla wystąpienia programu SQL Server w ramach programu DPM. Serwer raportów nasłuchuje żądań HTTP na porcie 80.
 - Włącz zdalne wywoływanie procedur w zdalnym programie SQL Server.
 - Domyślne wystąpienie aparatu bazy danych nasłuchuje na porcie TCP 1443. Ustawienie to można zmodyfikować. Aby można było używać usługi SQL Server Browser do łączenia z wystąpieniami, które nie nasłuchują na domyślnym porcie 1433, potrzebny będzie port UDP 1434.
 - Nazwane wystąpienie programu SQL Server domyślnie używa portów dynamicznych. Ustawienie to można zmodyfikować.

- o Numer bieżącego portu używanego przez aparat bazy danych jest widoczny w dzienniku błędów programu SQL Server. Dzienniki błędów można wyświetlać przy użyciu programu SQL Server Management Studio przez podłączenie do wystąpienia nazwanego. Bieżący dziennik można wyświetlić w obszarze Zarządzanie — dzienniki programu SQL Server w ramach wpisu Serwer nasłuchuje na porcie ['any' numer_portu].

NOTE

- Program DPM 2016 wymaga SQL Server Management Studio (SSMS) w wersji 16,5 lub starszej. Program SSMS nie jest już instalowany z SQL Server; musisz [pobrać i zainstalować program SQL Server Management Studio \(SSMS\) w wersji 16,5](#).
- Program SSMS w wersji 17,0 lub nowszej nie jest obsługiwany w programie DPM 2016. Aby uzyskać więcej informacji, zobacz [SQL Server Management Studio wersja 16,5](#).
- W przypadku programu DPM 2019 należy zainstalować program SQL SSRS osobno dla programu SQL 2017. W programie SQL 2017 i nowszych wersjach usługi SSRS nie są instalowane w ramach instalacji programu SQL Server. Aby uzyskać więcej informacji, zobacz [Install SQL Server Reporting Services \(2017 i nowsze\)](#).

Instalowanie programu DPM

IMPORTANT

Podczas instalowania programu DPM należy użyć nazw NetBIOS dla nazwy domeny i nazwy maszyny SQL. Nie należy używać w pełni kwalifikowanych nazw domen (FQDN).

1. W razie potrzeby Wyodrębnij plik DPM 2016. exe (w przypadku programu DPM 2016)/DPM 2019. exe (dla programu DPM 2019) na komputerze, na którym chcesz uruchomić program DPM. W tym celu uruchom plik exe i na ekranie **Welcome** (Witamy) kliknij pozycję **Next** (Dalej). Na ekranie **Select Destination Location** (Wybierz lokalizację docelową) określ, gdzie chcesz wyodrębnić pliki instalacyjne. Na ekranie **Ready to Extract** (Gotowe do wyodrębnienia) kliknij pozycję **Extract** (Wyodrębnij). Po zakończeniu wyodrębniania przejdź do określonej lokalizacji i uruchom plik **Setup.exe**.
2. Na stronie **Zapraszamy** instalatora programu DPM kliknij przycisk **Dalej**. Na stronie **Postanowienia licencyjne** zaakceptuj umowę i wybierz przycisk **OK**.
3. Na stronie **Sprawdzanie wymagań wstępnych** poczekaj na wykonanie sprawdzenia i przed kontynuowaniem rozwiąż wszelkie problemy.
4. Na stronie **Rejestracja produktu** kliknij przycisk **Dalej**. Na stronie **Zgoda na korzystanie z usługi Microsoft Update** zdecyduj, czy chcesz, aby program DPM był uwzględniany przez usługę Microsoft Updates.
5. Na stronie **Podsumowanie ustawień** sprawdź ustawienia i kliknij przycisk **Instaluj**. Po ukończeniu instalacji kliknij przycisk **Zamknij**. Automatycznie zostanie uruchomiona usługa Windows Update w celu wyszukania zmian.

Uruchamianie instalacji nienadzorowanej

Uruchom instalację nienadzorowaną w następujący sposób:

1. Przed rozpoczęciem upewnij się, że wstępnie wymagane składniki zostały zainstalowane.
2. Na SQL Server zdalnym upewnij się, że .NET Framework 3,5 (dla programu SQL 2016) 4,0 lub 4,5 (SQL 2017) jest zainstalowany w systemie Windows Server przed zainstalowaniem programu SQL.
3. Użyj następującego kodu, aby upewnić się, że zaporą jest otwarta:

```
netsh advfirewall firewall add rule name=DPM_SqlSrvr.exe dir=in action=allow
program="%PROGRAMFILES%\Microsoft SQL Server\MSSQL11.MSSQLSERVER\MSSQL\Binn\sqlservr.exe\"
profile=Domain
netsh advfirewall firewall add rule name=DPM_UDP_Port_1434 dir=in action=allow protocol=UDP
localport=1434 profile=Domain
```

4. Zainstaluj program SQL Server na serwerze lokalnym lub zdalnym.
5. Skopiuj poniższy tekst do Notatnika (lub innego edytora tekstu) i zapisz skrypt na serwerze programu DPM jako plik DPMSetup.ini. Ten sam skrypt będzie używany niezależnie od tego, czy wystąpienie programu SQL Server jest zainstalowane na serwerze DPM, czy też na serwerze zdalnym.

IMPORTANT

Podczas instalowania programu DPM należy użyć nazw NetBIOS dla nazwy domeny i nazwy maszyny SQL. Nie należy używać w pełni kwalifikowanych nazw domen (FQDN).

Podczas tworzenia pliku DPMSetup.ini tekst wewnątrz nawiasów ostrych (<>) należy zastąpić wartościami z własnego środowiska. Wiersze rozpoczynające się od znaku krzyżyka (#) są komentarzami i instalator programu DPM użyje wartości domyślnych. Aby określić własne wartości, wpisz wartości w nawiasach ostrych (<>) i usuń krzyżyk (#).

```
[OPTIONS]
UserName = <A user with credentials to install DPM>
CompanyName = <Name of your company>
ProductKey = <The 25-character DPM product key in the format xxxxx-xxxxx-xxxxx-xxxxx-xxxxx>
# SqlAccountPassword = <The password to the DPM$ account>
# StandardAgentLicenses = <No. of standard agent licenses you have purchased>
# EnterpriseAgentLicenses = <No. of enterprise agent licenses you have purchased>
# ProgramFiles = C:\Program Files\Microsoft Data Protection Manager
# DatabaseFiles = C:\Program Files\Microsoft Data Protection Manager\DPM\DPMDB
# IntegratedInstallSource = <Location of the DPM setup files>
# ---For using a remote SQL Server instance ---
# SQLMachineName = <Name of the SQL Server computer> OR <SQL Cluster Name>
# SQLInstanceName = <Name of the instance of SQL Server that Setup must use>
# SQLMachineUserName = <User name that Setup must use>
# SQLMachinePassword = <Password for the user name Setup must use>
# SQLMachineDomainName = <Domain to which the SQL Server computer is attached>
# ---For using a reporting SQL Server instance in case of DPMDB in SQL Cluster ---
# ReportingMachineName = <Name of the SQL Server computer>
# ReportingInstanceName = <Name of the instance of SQL Server that Setup must use, SSRS in case of
SQL 2017>
# ReportingMachineUserName = <User name that Setup must use>
# ReportingMachinePassword = <Password for the user name Setup must use>
# ReportingMachineDomainName = <Domain to which the SQL Server computer is attached>
```

6. Po zapisaniu pliku w wierszu polecenia z podwyższonym poziomem uprawnień na serwerze instalacji wpisz: `start /wait [media location]\setup.exe /i /f <path>\DPMSetup.ini /l <path>\dpmlog.txt`.
- `[media location]` wskazuje, gdzie będzie uruchamiany plik Setup. exe z programu.
 - `<path>` jest lokalizacją pliku ini.

Instalowanie programu DPM na kontrolerze domeny

Aby skonfigurować program DPM na kontrolerze RODC, przed skonfigurowaniem programu SQL Server i zainstalowaniem programu DPM należy wykonać kilka czynności.

1. Utwórz grupy zabezpieczeń i konta na potrzeby programu DPM. W tym celu kliknij pozycję **Start** >

Narzędzia administracyjne > Użytkownicy i komputery usługi Active Directory >

Domena/Built-in i utwórz te grupy zabezpieczeń. Dla każdej z grup użyj domyślnych ustawień zakresu (globalny) i typu grupy (zabezpieczenia):

- *Nazwa komputera*DPMDBReaders \$ < >;
- *Nazwa komputera*MSDPMTrustedMachines \$ < >;
- *Nazwa komputera*DPMRADCOMTrustedMachines \$ < >;
- *Nazwa komputera*DPMRADmTrustedMachines \$ < >;
- *Nazwa komputera*DPMDBAdministrators \$ < >;
- *Nazwa komputera*MSDPMTrustedUsers \$ < >;
- *Nazwa komputera*DPMSCOM \$ < >;
- DPMRATrustedDPMRAs \$ <*Nazwa komputera*>, gdzie <*Nazwa komputera*> to nazwa kontrolera domeny.

2. Dodaj konto komputera lokalnego dla kontrolera domeny (<*Nazwa komputera*>) do grupy MSDPMTrustedMachines\$<*Nazwa komputera*>. Następnie na podstawowym kontrolerze domeny utwórz konto użytkownika domeny z poświadczeniami o możliwie najniższym poziomie. Przypisz do niego silne hasło, które nie wygasa, i dodaj je do lokalnej grupy administratorów.

NOTE

To konto należy zapamiętać, ponieważ podczas instalacji programu SQL Server trzeba będzie skonfigurować usługi programu SQL Server. To konto użytkownika można nazwać w dowolny sposób, jednak aby z łatwością rozpoznawać jego przeznaczenie, warto nadać mu znaczącą nazwę — taką jak DPMSQLSvcsAcct. Dla celów tych procedur to konto będzie nazwane DPMSQLSvcsAcct.

3. Na podstawowym kontrolerze domeny utwórz kolejne konto użytkownika domeny z poświadczeniami o możliwie najniższym poziomie, nazwij je DPMR\$MACHINENAME, przypisz do niego silne hasło, które nie wygasa, a następnie dodaj to konto do grupy DPMDBReaders\$<*Nazwa komputera*>.
4. Następnie utwórz grupy zabezpieczeń i konta użytkowników na potrzeby bazy danych programu SQL Server z ustawieniem zakresu: globalny i typem grupy: zabezpieczenia. W tym formacie Grupa lub konto ma <grouporaccountnameComputerName>.
 - SQLServerSQL2005BrowserUser\$<*Nazwa komputera*>
 - SQLServerMSSQLServerADHelperUser\$<*Nazwa komputera*>
 - SQLServerReportServerUser\$<*Identyfikator wystąpienia*> <*Nazwa wystąpienia*>
 - SQLServerMSASUser\$<*Nazwa komputera*> <*Nazwa wystąpienia*>
 - SQLServerDTSUser\$<*Nazwa komputera*>
 - SQLServerFDHostUser<*Nazwa komputera*> <*Nazwa wystąpienia*>
 - gdzie <*Nazwa komputera*> to nazwa komputera kontrolera domeny, na którym ma zostać zainstalowany program SQL Server 2008.
 - <*Nazwa wystąpienia*> to nazwa wystąpienia programu SQL Server, które ma zostać utworzone na kontrolerze domeny. Nazwą wystąpienia może być dowolna nazwa inna niż domyślna nazwa wystąpienia programu DPM (MSDPM2010).
 - <*Identyfikator wystąpienia*> jest domyślnie przypisywany przez Instalatora programu SQL Server. Informuje, że grupa ma zastosowanie do usług Reporting Services (MSRS) dla wersji głównej wystąpienia (10) programu SQL Server. W tym wydaniu ta wartość to MSRS1A0_50.
5. Na podstawowym kontrolerze domeny dodaj utworzone wcześniej konto użytkownika domeny (konto

DPMSQLSvcAcct) do następujących grup: SQLServerReportServerUser\$ <Nazwa komputera>\$MSRS10.<Identyfikator wystąpienia> SQLServerMSASUser\$ <Nazwa komputera>\$<Identyfikator wystąpienia>

6. Po wykonaniu tych kroków możesz zainstalować program SQL Server:

- Zaloguj się na kontrolerze domeny, na którym chcesz zainstalować program DPM przy użyciu utworzonego wcześniej konta użytkownika domeny. Będziemy nazywać to konto DPMSQLSvcAcct.
- Rozpocznij instalację programu SQL Server. Na stronie **Konfiguracja serwera — Konta usług** instalatora musisz podać konto logowania dla usług programu SQL Server (agent programu SQL Server, aparat bazy danych programu SQL Server i usługi SQL Server Reporting Services), aby były uruchamiane na koncie użytkownika DPMSQLSvcAcct.
- Po zainstalowaniu programu SQL Server otwórz pozycję **SQL Server Configuration Manager** > **Konfiguracja sieci programu SQL Server** > **Protokoły** i kliknij prawym przyciskiem myszy pozycję **Nazwane potoki** > **Włącz**. Musisz zatrzymać i ponownie uruchomić usługę programu SQL Server.

7. Następnie możesz zainstalować program DPM:

- Na stronie **Ustawienia programu SQL Server** wpisz nazwę wystąpienia programu SQL Server zainstalowanego w procedurze jako localhost\<Nazwa wystąpienia>, a następnie wpisz poświadczenia pierwszego utworzonego konta użytkownika domeny (konto DPMSQLSvcAcct). To konto musi być członkiem lokalnej grupy administratorów na kontrolerze domeny, na którym jest zainstalowane wystąpienie zdalne. Po zakończeniu instalacji można usunąć konto użytkownika z lokalnej grupy administratorów.
- Na stronie **Ustawienia zabezpieczeń** trzeba będzie wprowadzić to samo hasło, które zostało użyte wcześniej do utworzenia konta użytkownika DPMR\$MACHINEName.
- Otwórz program SQL Server Management Studio i połącz się z wystąpieniem programu SQL Server, do którego używania jest skonfigurowany program DPM. Kliknij pozycję **nowe zapytanie**, Skopiuj poniższy tekst do okienka po prawej stronie, a następnie naciśnij klawisz F5, aby uruchomić zapytanie.

```
use DPMDB
declare @refresh_jobid uniqueidentifier
select @refresh_jobid = ScheduleId from tbl_SCH_ScheduleDefinition where JobDefinitionId in
(select JobDefinitionId from tbl_JM_TaskDefinition where TaskDefinitionId in (select distinct
TaskDefinitionID from tbl_TE_TaskTrail
where VerbID = '53603503-C4C8-4D0E-8F1E-D2F3868E51E3')) and IsDeleted=0
exec msdb.dbo.sp_update_job @job_name =@refresh_jobid, @enabled=0
update tbl_SCH_ScheduleDefinition
set IsDeleted=1
where ScheduleId = @refresh_jobid
```

Uaktualnij program SQL 2016 do wersji SQL 2017

Jeśli chcesz użyć programu SQL 2017 z półrocznym kanałem programu DPM 1801 lub nowszym, musisz uaktualnić SQL 2016 do programu SQL 2017. Do programu SQL 2017 można uaktualnić SQL Server 2016 lub SQL Server 2016 SP1 Enterprise lub standard. Poniższa procedura zawiera listę czynności, które należy wykonać, aby uaktualnić program SQL 2016 do programu SQL 2017.

NOTE

Program SQL 2017 jest obsługiwany jako baza danych programu DPM 1801 w scenariuszach uaktualniania. W przypadku programu DPM 2019 program SQL 2017 jest obsługiwany jako DPM database w ramach nowych scenariuszy instalacji i uaktualniania programu DPM.

1. Na SQL Server wykonaj kopię zapasową bazy danych raportowania.
2. Wykonaj kopię zapasową kluczy szyfrowania.
3. Wyczyść foldery raportowania na komputerze lokalnym.
4. Zainstaluj usługę raportowania.
5. Na serwerze programu DPM Zmień następujący klucz rejestru programu DPM na nową nazwę wystąpienia raportowania.
 - HKEY_LOCAL_MACHINE \SOFTWARE\Microsoft\Microsoft Data Protection Manager\DB<ReportingInstanceName>
6. Zmień nazwę katalogu wirtualnego usługi Reporting Services na ReportServer_SSRS.
7. Skonfiguruj usługę raportowania i Przywróć bazę danych i klucze szyfrowania.

Uaktualnianie instalacji programu DPM

11.12.2019 • 60 minutes to read

Ten artykuł zawiera informacje o uaktualnianiu programu System Center 2019 — Data Protection Manager (DPM).

Uaktualnianie do programu DPM 2019

Program System Center-2019 Data Protection Manager (DPM) można zainstalować w systemie Windows Server 2016 lub 2019. Program DPM 2019 można uaktualnić z następujących wersji:

- DPM 2016
- DPM 1801
- DPM 1807

Przed przeprowadzeniem uaktualnienia do programu DPM 2019 lub jego instalacji przeczytaj temat [wymagania wstępne instalacji](#).

Ścieżka uaktualnienia programu DPM 2019

W przypadku uaktualniania programu DPM 2016 do programu DPM 2019 upewnij się, że instalacja obejmuje następujące wymagane aktualizacje:

- Uaktualnij serwer programu DPM do wersji DPM 2019.
- Zaktualizuj agentów na serwerach chronionych.
- Uaktualnij administratora zdalnego programu DPM na wszystkich serwerach produkcyjnych.
- Kopie zapasowe są kontynuowane bez ponownego uruchamiania serwera produkcyjnego.

Procedura uaktualniania programu DPM

1. Aby zainstalować program DPM, kliknij dwukrotnie plik Setup. exe, aby otworzyć Kreatora programu System Center 2019.
2. W obszarze Instalacja kliknij przycisk Data Protection Manager, aby uruchomić Kreatora instalacji. Zaakceptuj warunki i postanowienia licencyjne, a następnie wykonaj kroki Kreatora instalacji.

Instrukcje dotyczące instalowania programu DPM znajdują się w artykule [Instalowanie programu DPM](#).

Migrowanie DPM database podczas uaktualniania

W ramach uaktualniania możesz przenieść bazę danych DPM. Na przykład:

- Scalasz wystąpienia SQL Server.
- Jeśli wykonujesz przeniesienie do zdalnego programu SQL Server o wyższej wydajności.
- Jeśli chcesz dodać odporność na uszkodzenia za pomocą klastra programu SQL Server lub wykonać przeniesienie między zdalnym i lokalnym programem SQL Server w dowolną stronę.

Instalator programu DPM 2019 umożliwia migrowanie DPM database do różnych serwerów SQL podczas uaktualniania.

Możliwe scenariusze migracji bazy danych

Podczas uaktualniania programu DPM 2016/1801/1807 do programu DPM 2019 istnieją następujące

scenariusze:

1. Lokalne wystąpienie i migracja do zdalnego wystąpienia SQL Server podczas instalacji.
2. Wystąpienie zdalne i migracja do lokalnego wystąpienia SQL Server podczas instalacji.
3. Wystąpienie lokalne i migracja do zdalnego wystąpienia klastra SQL Server podczas instalacji.
4. Lokalne wystąpienie i migracja do innego lokalnego wystąpienia SQL Server podczas instalacji.
5. Zdalne wystąpienie i migracja do innego zdalnego wystąpienia SQL Server podczas instalacji.
6. Wystąpienie zdalne i migracja do zdalnego wystąpienia klastra SQL Server podczas instalacji.

Przygotowanie do migracji bazy danych

Jeśli chcesz użyć nowego programu SQL Server do migrowania DPM database, przed uaktualnieniem programu DPM upewnij się, że oba serwery SQL mają takie same:

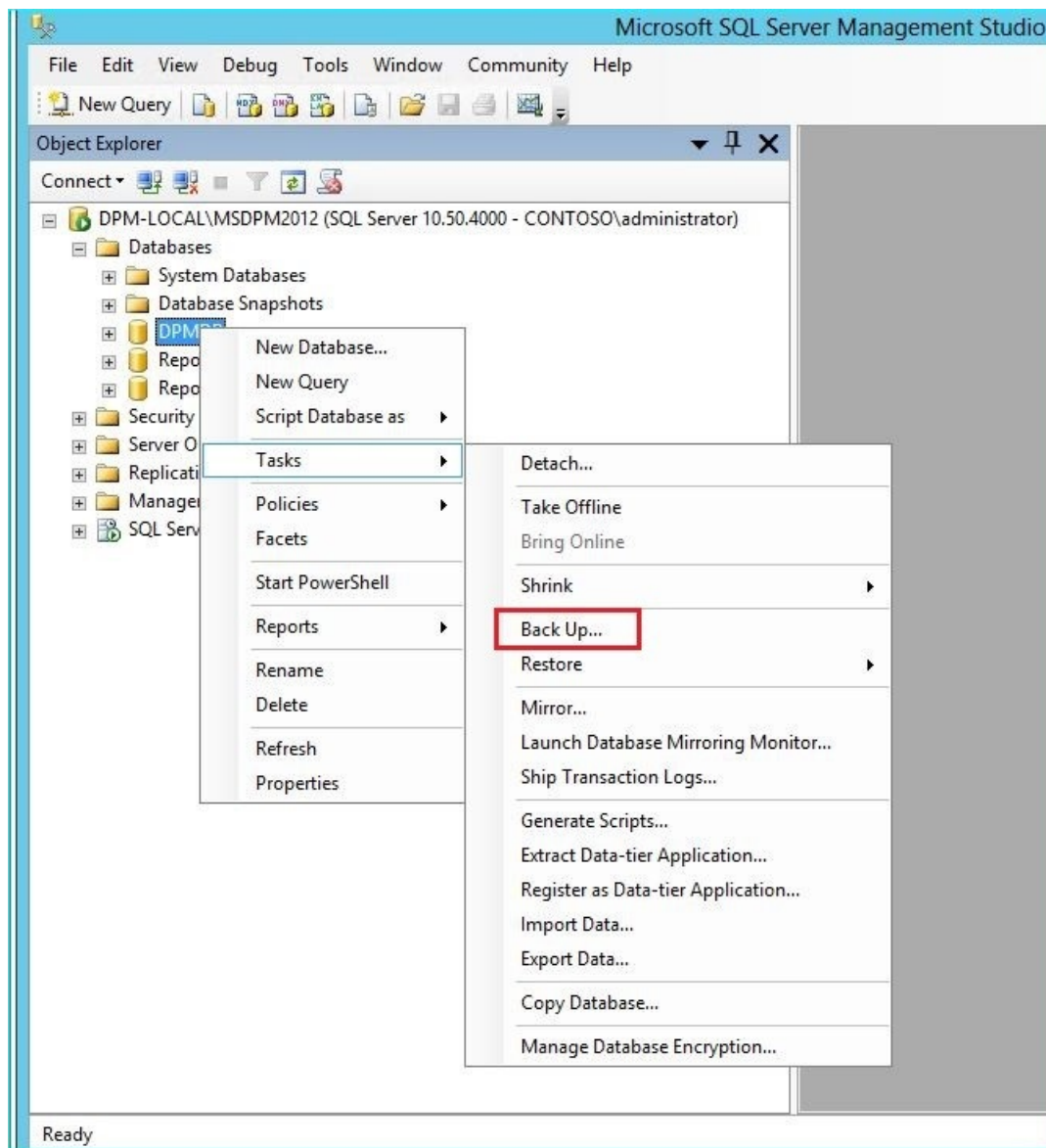
- Wymagania dotyczące programu SQL Server
- Konfiguracja konfiguracji
- Reguły zapory
- Pliki obsługi programu DPM ()

Gdy nowe wystąpienie SQL Server zainstalowane i przygotowane do użytku programu DPM, należy wykonać kopię zapasową bieżącego DPM database i przywrócić je na nowym SQL Server.

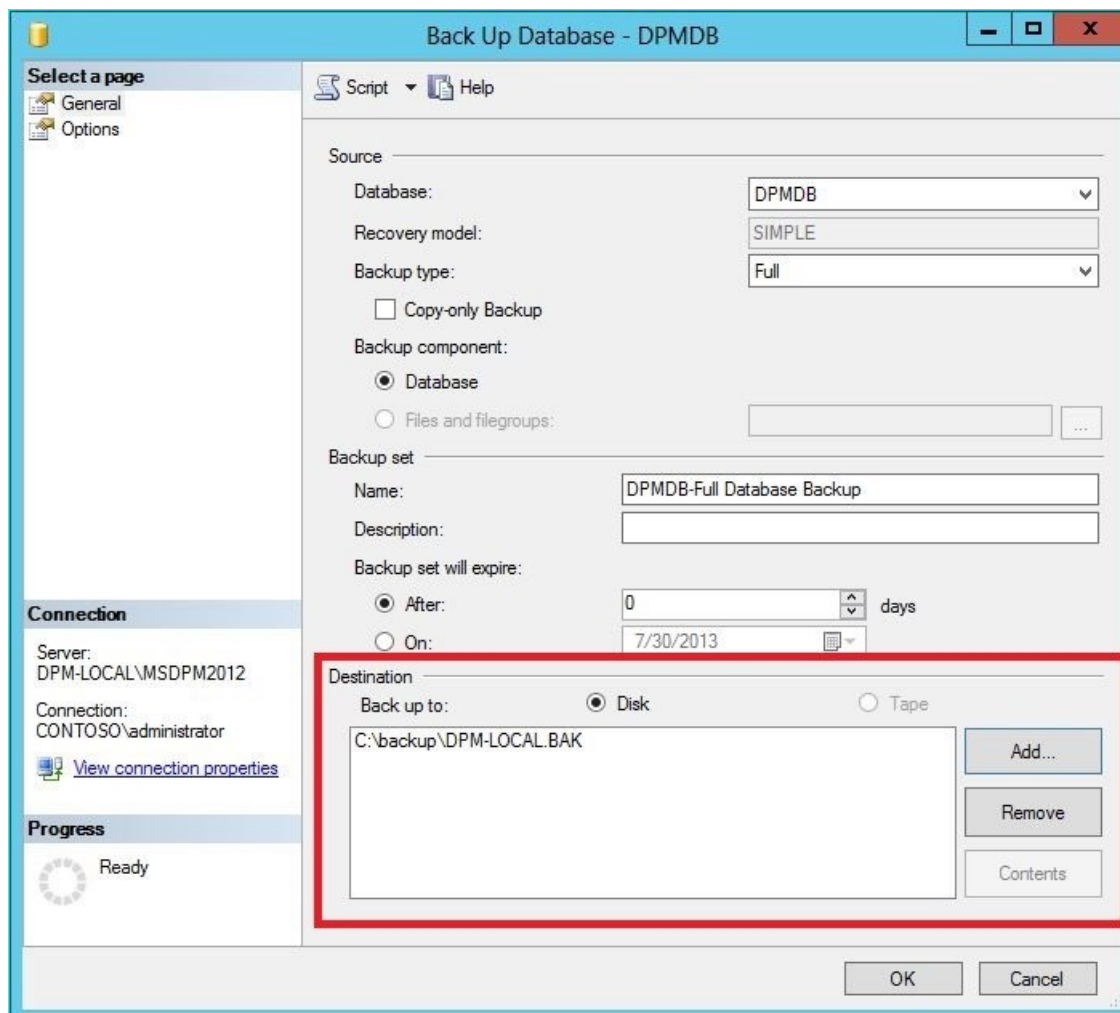
Kroki przed uaktualnieniem: Tworzenie kopii zapasowej i przywracanie bazy danych programu DPM 2016/1801/1807 do nowego wystąpienia SQL

Ten przykład przygotowuje zdalny klaster SQL Server do użycia podczas migracji.

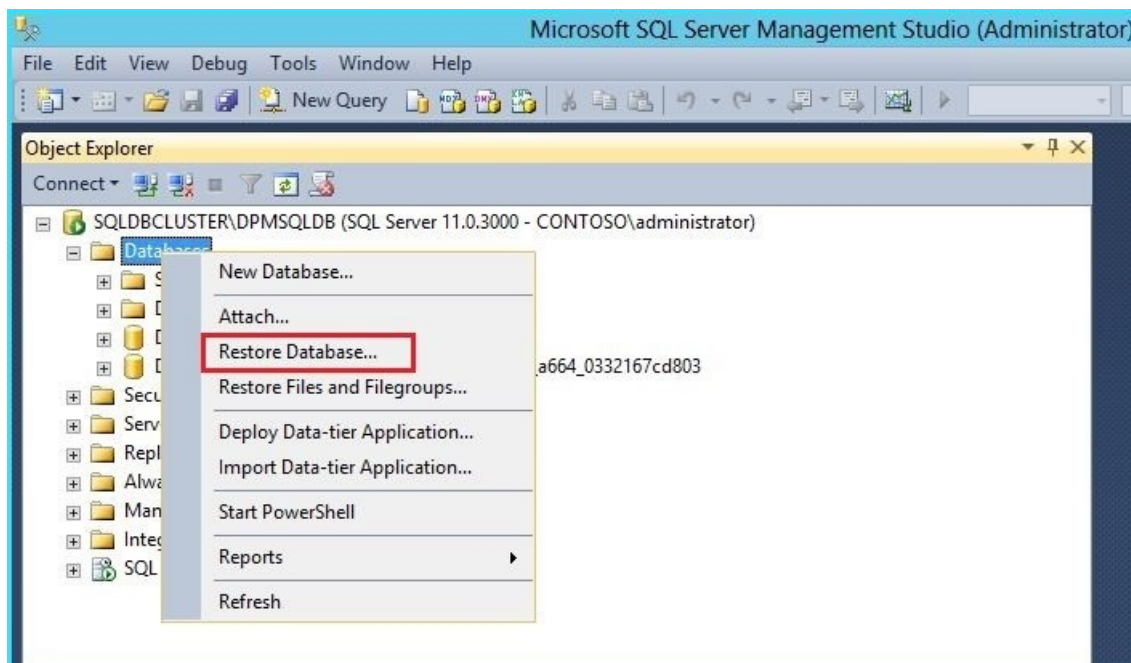
1. Na serwerze programu System Center Data Protection Manager lub na SQL Server zdalnym hostującym DPM database Uruchom **program Microsoft SQL Management Studio** i Połącz się z wystąpieniem programu SQL HOSTUJĄCYM bieżące DPMDb programu DPM.
2. Kliknij prawym przyciskiem myszy bazę danych DPM i w obszarze **Zadania** wybierz pozycję **Utwórz kopię zapasową...** .



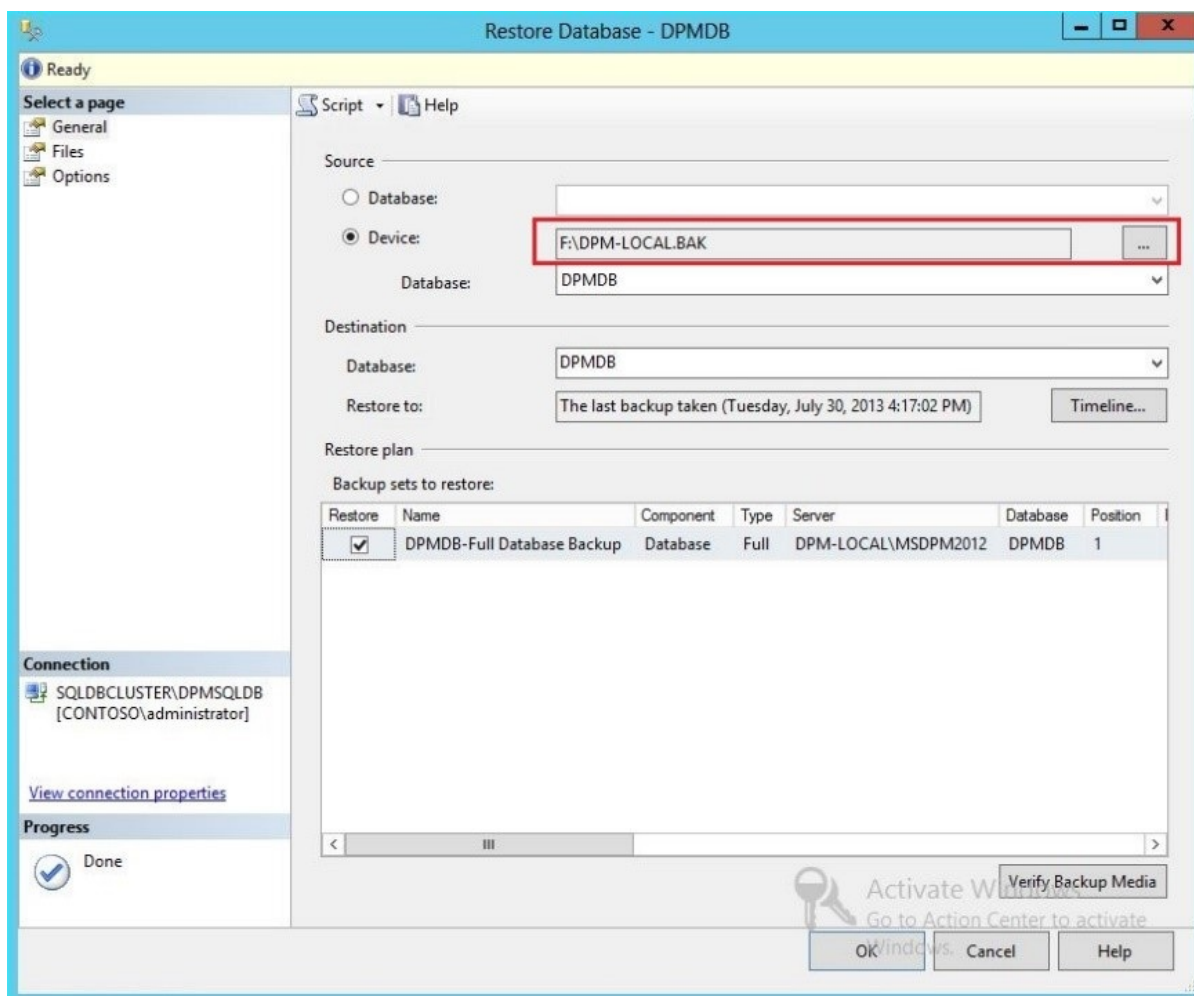
3. Dodaj miejsce docelowe kopii zapasowej i nazwę pliku, a następnie wybierz pozycję **OK**, aby rozpocząć tworzenie kopii zapasowej.



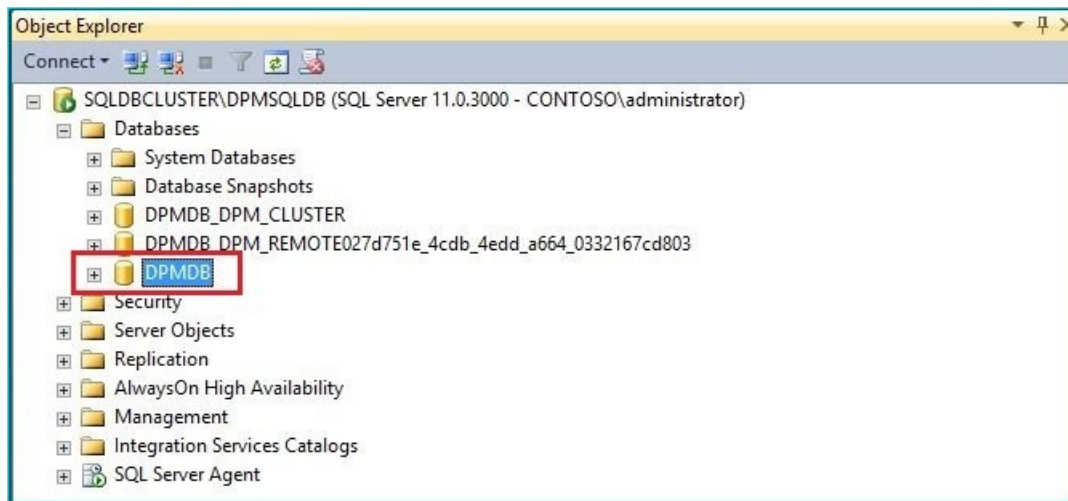
4. Po wykonaniu kopii zapasowej skopiuj plik wyjściowy do zdalnego programu SQL Server. Jeśli jest to klaster programu SQL, skopiuj go do aktywnego węzła hostującego wystąpienie programu SQL, którego chcesz użyć podczas uaktualniania programu DPM. Przed przystąpieniem do przywracania DPM database należy skopiować go na dysk udostępnionego klastra.
5. Na maszynie zdalnego programu SQL Server uruchom program **Microsoft SQL Management Studio** i połącz się z wystąpieniem programu SQL, którego chcesz użyć podczas uaktualniania programu DPM. Jeśli jest to klaster programu SQL, należy to zrobić w aktywnym węźle, do którego skopiowano plik kopii zapasowej. Plik kopii zapasowej teraz powinien znajdować się na udostępnionym dysku klastra.
6. Kliknij prawym przyciskiem myszy ikonę Bazy danych, a następnie wybierz polecenie **Przywróć bazę danych...**. Spowoduje to uruchomienie kreatora przywracania.



7. Wybierz pozycję **Urządzenie** w obszarze **Źródło**, a następnie znajdź plik kopii zapasowej bazy danych, który został skopiowany w poprzednim kroku, i wybierz go. Zweryfikuj opcje i lokalizację przywracania, a następnie wybierz pozycję **OK**, aby rozpocząć przywracanie. Rozwiąż wszelkie problemy zgłoszone podczas przywracania, aby zakończyć je pomyślnie.



8. Po zakończeniu przywracania przywrócona baza danych będzie widoczna w obszarze **bazy danych** z oryginalną nazwą. Ta baza danych zostanie użyta podczas uaktualniania. Możesz wyjść z programu **Microsoft SQL Management Studio** i rozpocząć proces uaktualniania na oryginalnym serwerze DPM.



9. Jeśli nowy serwer SQL jest zdalnym serwerem SQL, zainstaluj narzędzia do zarządzania SQL na serwerze programu DPM. Wersja narzędzi zarządzania programem SQL musi pasować do wersji programu SQL Server hostującego bazę danych DPMDB.

Rozpocznij uaktualnienie, aby zmigrować DPMDB do innego SQL Server

NOTE

Jeśli wystąpienie programu SQL jest współużytkowane, uruchom instalację lub uaktualnienia programu DPM sekwencyjnie. Instalowanie równoległe może spowodować wystąpienie błędów.

1. Po zakończeniu czynności przygotowujących przed migracją Uruchom proces instalacji programu DPM 2019. Instalator programu DPM pokazuje informacje o bieżącym wystąpieniu programu SQL Server, które zostało wstępnie wypełnione. Jest to miejsce, w którym można wybrać inne wystąpienie programu SQL Server lub zmienić klastrowane wystąpienie programu SQL używane podczas migracji.

Data Protection Manager Setup

Prerequisites Check

Please wait while the wizard checks for required hardware and software.

Installation Stages

- Welcome
- Prerequisites check
- Product registration
- Installation settings
- Microsoft Update Opt-In
- Customer feedback option
- Installation

DPM requires a database. You can use a local or remote instance of SQL Server that already exists.

☒ Use stand-alone SQL Server.
SQL Server is not clustered.

☐ Use clustered SQL Server
SQL Server is clustered

Instance of SQL Server
(Example: SQLSERV or SQLSERV\MYSQLINSTANCE):

User Name: Password:

Domain:

Select the appropriate option and click on the button to perform the prerequisite check and install the missing Windows components.

< Back Next > Cancel Help

2. Zmień ustawienia SQL, aby użyć wystąpienia programu SQL Server, do którego przywrócono bazę danych programu DPM. Jeśli jest to klaster programu SQL, musisz także określić osobne wystąpienie programu SQL Server używane na potrzeby raportowania programu SQL. Przyjęto, że wszystkie reguły zapory oraz program SQLPrep zostały już uruchomione. Musisz podać poprawne poświadczenia, a następnie kliknąć przycisk **Sprawdź i instaluj**.

Data Protection Manager Setup

Prerequisites Check

Please wait while the wizard checks for required hardware and software.

Installation Stages

- Welcome
- Prerequisites check**
- Product registration
- Installation settings
- Microsoft Update Opt-In
- Customer feedback option
- Installation

DPM requires a database. You can use a local or remote instance of SQL Server that already exists.

☐ Use stand-alone SQL Server.
 SQL Server is not clustered.

☒ Use clustered SQL Server
 SQL Server is clustered

Instance of SQL Server
 (Example: SQLSERV or SQLSERV\MYSQLINSTANCE):

User Name: Password:

Domain:

Instance of SQL Server Reporting Service
 (Example: SQLSERV or SQLSERV\MYREPORTINGINSTANCE):

User Name: Password:

Domain:

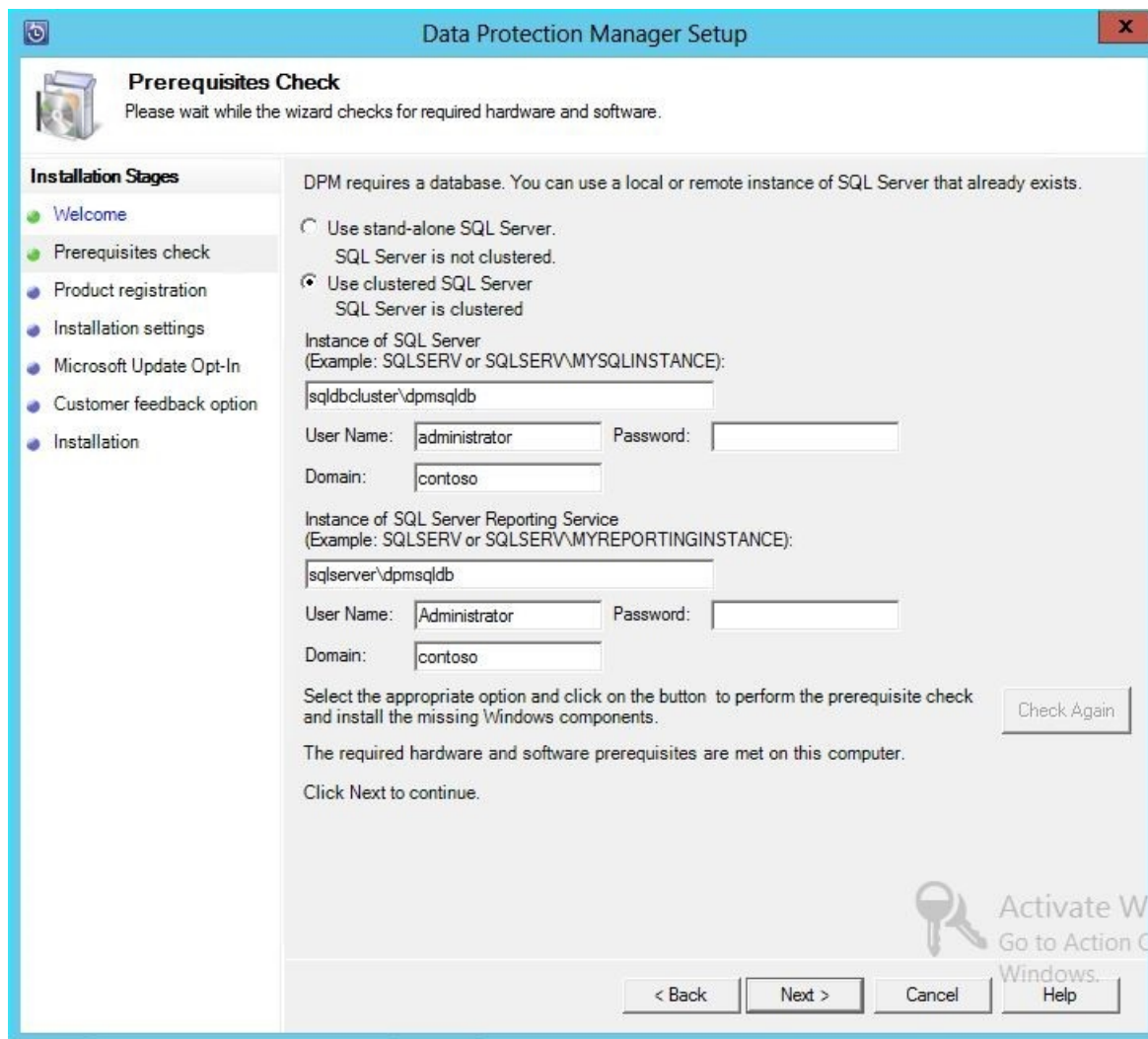
Select the appropriate option and click on the button to perform the prerequisite check and install the missing Windows components.

Check and Install

Details

Setup will use the current user's credentials for this SQL instance.

3. Sprawdzanie wymagań wstępnych powinno zakończyć się pomyślnie, kliknij przycisk **dalej** , aby kontynuować uaktualnianie.



4. Kontynuuj pracę z opcjami kreatora i Ukończ instalację.
5. Po zakończeniu instalacji odpowiednia nazwa bazy danych w określonym wystąpieniu zostanie teraz *DMPMB_DPMServerName*. Ponieważ może być współużytkowane z innymi serwerami programu DPM, Konwencja nazewnictwa DPM database będzie teraz: *DPM2016 \$ DPMDB_DPMServerName*

Dodawanie magazynu dla Nowoczesny magazyn kopii zapasowych

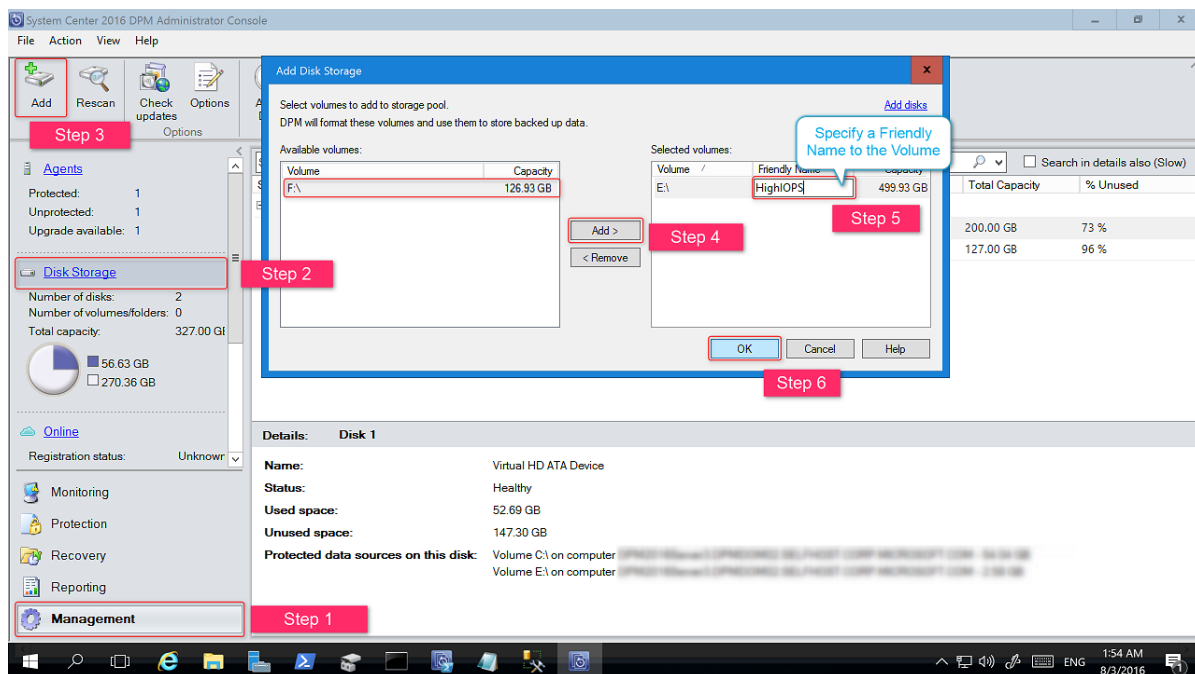
Aby efektywnie przechowywać kopie zapasowe, program DPM 2019 używa woluminów. Dysków można także używać do kontynuowania zapisywania kopii zapasowych.

Dodawanie woluminów i dysków

W przypadku uruchomienia programu DPM 2019 w systemie Windows Server można używać woluminów do przechowywania danych kopii zapasowej. Woluminy pozwalają zaoszczędzić miejsce do magazynowania i zapewniają szybsze tworzenie kopii zapasowych. Możesz nadać woluminowi przyjazną nazwę i możesz zmienić jego nazwę. Podczas dodawania woluminu lub później można zastosować przyjazną nazwę, wybierając kolumnę **przyjaznej nazwy** żadanego woluminu. Za pomocą programu PowerShell także można dodawać i zmieniać przyjazne nazwy dla woluminów.

Aby dodać wolumin w konsoli administratora:

1. W konsoli administratora programu DPM wybierz funkcję **Zarządzanie**, a następnie wybierz pozycję **Magazyn dyskowy > Dodaj**.
2. W oknie dialogowym **dodawanie Disk Storage** wybierz dostępny wolumin > kliknij przycisk **Dodaj** > Wpisz przyjazną nazwę woluminu > kliknij przycisk **OK**.



Jeśli chcesz dodać dysk, musi on należeć do grupy ochrony ze starszą wersją magazynu. Te dyski mogą być używane tylko dla tych grup ochrony. Jeśli serwer programu DPM nie ma źródeł ze starszą ochroną, dysk nie będzie widoczny. Aby uzyskać więcej informacji na temat dodawania dysków, zobacz [Dodawanie dysków w celu zwiększenia miejsca w starszej wersji magazynu](#). Dyskowi nie można nadać przyjaznej nazwy.

Przypisywanie obciążeń do woluminów

Program DPM 2019 pozwala określić typy obciążeń, które mają być przypisane do określonych woluminów. Na przykład drogie woluminy obsługujące dużą liczbę IOPS można skonfigurować do przechowywania tylko obciążeń wymagających częstego tworzenia kopii zapasowych o dużych ilościach, takich jak SQL z dziennikami transakcji.

Aby zaktualizować właściwości woluminu w puli magazynów na serwerze programu DPM, użyj polecenia cmdlet programu PowerShell *Update-DPMDiskStorage*.

Update-DPMDiskStorage

Składnia

Parameter Set: Volume

```
Update-DPMDiskStorage [-Volume] <Volume> [[-FriendlyName] <String> ] [[-DatasourceType] <VolumeTag[]> ] [-Confirm] [-WhatIf] [ <CommonParameters>]
```

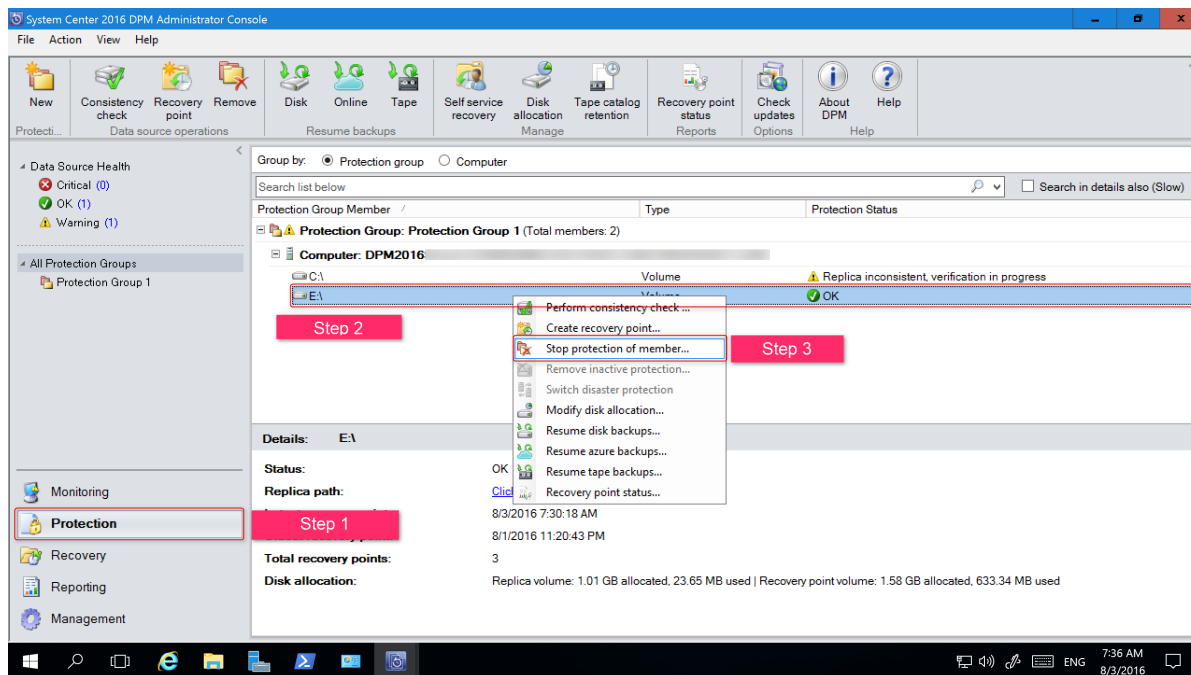
Zmiany wprowadzone za pomocą programu PowerShell są odzwierciedlane w interfejsie użytkownika.

Migrowanie starszej wersji magazynu do Nowoczesny magazyn kopii zapasowych

Po uaktualnieniu do programu DPM 2019 i systemu operacyjnego do systemu Windows Server 2016/2019 można zaktualizować istniejące grupy ochrony do nowych funkcji w programie 2016 DPM. Domyślnie grupy ochrony nie są zmieniane i nadal działają tak, jak zostały skonfigurowane we wcześniejszej wersji programu DPM. Opcjonalnie można zaktualizować grupy ochrony, aby używać Nowoczesny magazyn kopii zapasowych, jest opcjonalne. Aby zaktualizować grupę ochrony, Zatrzymaj ochronę wszystkich źródeł danych za pomocą opcji **Zachowaj dane**, a następnie Dodaj źródła danych do nowej grupy ochrony. Program DPM zacznie chronić te źródła danych w nowy sposób.

Wykonaj następujące czynności:

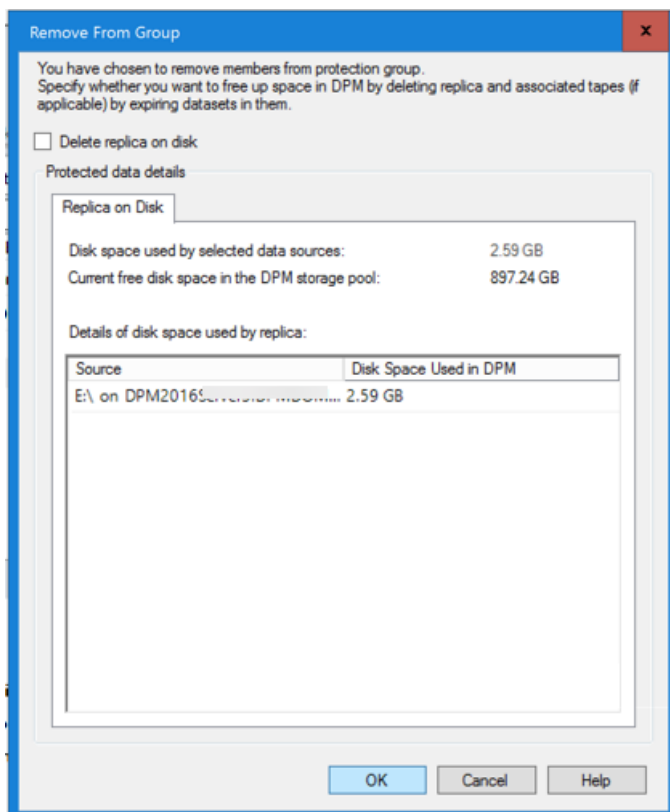
1. W konsoli administratora wybierz funkcję **Ochrona** i na liście **Element członkowski grupy ochrony** kliknij prawym przyciskiem myszy wybrany element członkowski, a następnie wybierz polecenie **Zatrzymaj ochronę elementu członkowskiego**.



Zostanie otwarte okno dialogowe **Usuń z grupy**.

2. W oknie dialogowym **Usuń z grupy** przejrzyj używane miejsce na dysku i dostępne wolne miejsce w puli magazynów. Domyślnie punkty odzyskiwania pozostają na dysku i wygasają zgodnie ze skojarzonymi z nimi zasadami przechowywania. Kliknij przycisk **OK**.

Aby natychmiast przywrócić zajęte miejsce na dysku do wolnej puli magazynów, zaznacz opcję **Usuń replikę z dysku**. Spowoduje to usunięcie danych kopii zapasowej (i punktów odzyskiwania) skojarzonych z tym elementem członkowskim.



3. Utwórz nową grupę ochrony, która używa Nowoczesny magazyn kopii zapasowych i Uwzględnij

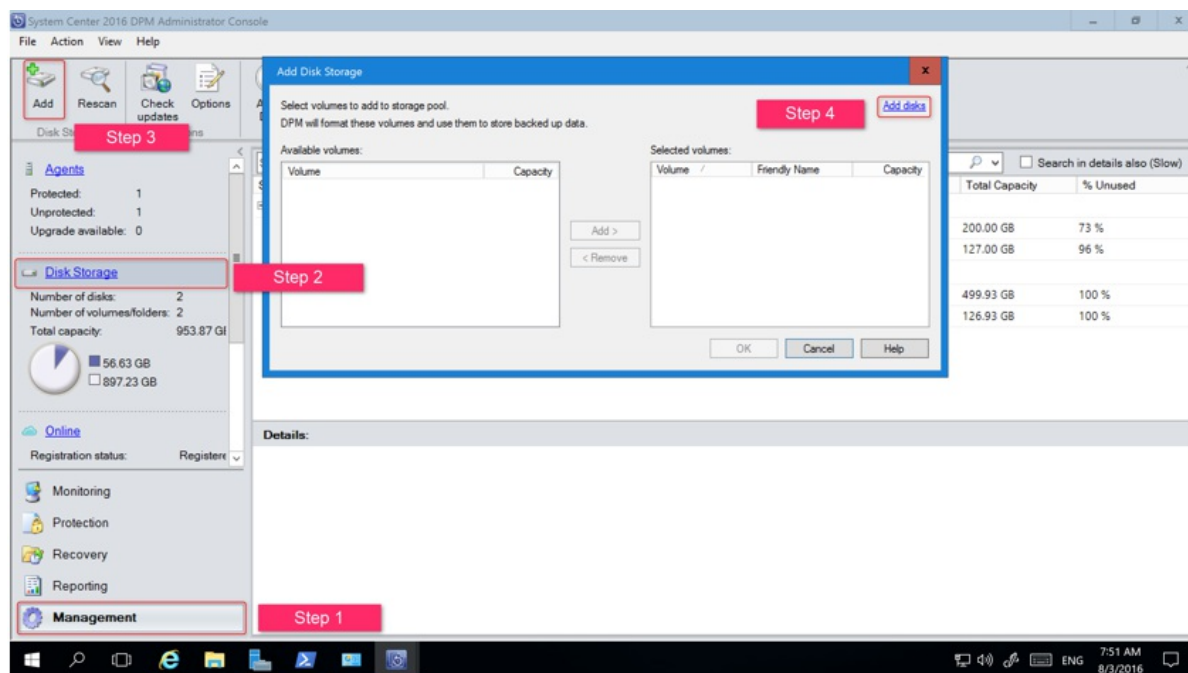
niechronione źródła danych.

Dodawanie dysków w celu zwiększenia ilości miejsca w starszej wersji

Jeśli chcesz używać starszej wersji magazynu z programem DPM 2019, może być konieczne dodanie dysków w celu zwiększenia starszej wersji magazynu. Aby dodać magazyn dyskowy:

1. W konsoli administratora kliknij pozycję **Zarządzanie**.
2. Wybierz pozycję **Magazyn dyskowy**.
3. Na wstążce narzędzi kliknij pozycję **Nowy**.

Zostanie otwarte okno dialogowe **Dodawanie magazynu dyskowego**.



4. W oknie dialogowym **Dodawanie magazynu dyskowego** kliknij pozycję **Dodaj dyski**.

Program DPM wyświetli listę dostępnych dysków.

5. Wybierz dyski, kliknij przycisk **Dodaj**, aby dodać te dyski, a następnie kliknij przycisk **OK**.

Włączanie ochrony w chmurze

Kopię zapasową serwera programu DPM można utworzyć na platformie Azure. Ogólna procedura jest następująca:

- Utwórz subskrypcję platformy Azure,
- Zarejestruj serwer w usłudze Azure Backup,
- Pobierz poświadczenia magazynu i agenta Azure Backup
- Skonfiguruj poświadczenia magazynu serwera i zasady tworzenia kopii zapasowych,

Aby uzyskać więcej informacji na temat tworzenia kopii zapasowych programu DPM w chmurze, zapoznaj się z artykułem [przygotowanie do tworzenia kopii zapasowych obciążeń na platformie Azure przy użyciu programu DPM](#).

Ten artykuł zawiera informacje o uaktualnianiu programu System Center 1807 — Data Protection Manager (DPM).

Aktualizacja do programu DPM 1807

Program System Center Data Protection Manager (DPM 1807) można zaktualizować tylko w programie DPM 1801. Program DPM 1807 to druga wersja w półroczu kanału programu System Center. Jeśli chcesz zaktualizować program DPM 1807 z programu DPM 2016, musisz najpierw zainstalować program DPM 1801, wykonując kroki opisane w artykule [Uaktualnianie instalacji programu DPM](#).

Kroki aktualizacji dla programu DPM 1807

1. Aby zainstalować program DPM, kliknij dwukrotnie plik Setup. exe, aby otworzyć Kreatora programu System Center 1807.
2. W obszarze Instalacja kliknij przycisk Data Protection Manager, aby uruchomić Kreatora instalacji. Zaakceptuj warunki i postanowienia licencyjne, a następnie wykonaj kroki Kreatora instalacji.

Ten artykuł zawiera informacje o uaktualnianiu programu System Center 1801 — Data Protection Manager (DPM).

Uaktualnianie do programu DPM 1801

Program System Center Data Protection Manager (DPM) można zainstalować w systemie Windows Server 2012 R2 lub Windows Server 2016 w wersji 1801. Program DPM 1801 to pierwsza wersja w półroczu kanału programu System Center. Uaktualnienie do programu DPM 1801 można przeprowadzić z programu DPM 2012 R2 z pakietem zbiorczym aktualizacji 14 (UR14) lub z programu DPM 2016 pakiet zbiorczy aktualizacji 4 (UR4). Przed uaktualnieniem lub zainstalowaniem programu DPM 2016 zapoznaj się z [wymaganiami wstępnymi instalacji](#).

Ścieżka uaktualnienia programu DPM 1801

Jeśli zamierzasz przeprowadzić uaktualnienie z programu DPM 2012 R2 lub DPM 2016 do programu DPM 1801, upewnij się, że instalacja ma wymagane aktualizacje:

- Uaktualnij program DPM 2012 R2 do programu DPM 2012 R2 z pakietem zbiorczym aktualizacji 14. Jeśli uaktualniasz program DPM 2016, najpierw Uaktualnij program do wersji DPM 2016 Update Rollup 4. Pakiety zbiorcze aktualizacji można pobrać z programu Windows Update.
- Uaktualnij serwer programu DPM do wersji DPM 1801.
- Zaktualizuj agentów na serwerach chronionych.
- Uaktualnij administratora zdalnego programu DPM na wszystkich serwerach produkcyjnych.
- Kopie zapasowe są kontynuowane bez ponownego uruchamiania serwera produkcyjnego.

Procedura uaktualniania programu DPM

1. Aby zainstalować program DPM, kliknij dwukrotnie plik Setup. exe, aby otworzyć Kreatora programu System Center 1801.
2. W obszarze Instalacja kliknij przycisk Data Protection Manager, aby uruchomić Kreatora instalacji. Zaakceptuj warunki i postanowienia licencyjne, a następnie wykonaj kroki Kreatora instalacji.

Niektóre funkcje programu DPM 1801, takie jak Nowoczesny magazyn kopii zapasowych, wymagają systemu Windows Server 2016. Program DPM 1801 można uruchomić w systemie Windows Server 2012 R2 z UR14. Aby jednak korzystać z funkcji, takich jak Nowoczesny magazyn kopii zapasowych lub kopia zapasowa maszyny wirtualnej funkcji Hyper-V opartych na RCT, należy użyć systemu Windows Server 2016. Instrukcje dotyczące instalowania programu DPM znajdują się w artykule [Instalowanie programu DPM](#).

Migrowanie bazy danych DPM podczas uaktualniania

W ramach uaktualniania możesz przenieść bazę danych DPM. Na przykład w przypadku scalania wystąpień programu SQL Server. Jeśli wykonujesz przeniesienie do zdalnego programu SQL Server o wyższej wydajności.

Jeśli chcesz dodać odporność na uszkodzenia za pomocą klastra programu SQL Server lub wykonać przeniesienie między zdalnym i lokalnym programem SQL Server w dowolną stronę. Instalator programu DPM 1801 umożliwia migrowanie DPM database do różnych serwerów SQL podczas uaktualniania.

Możliwe scenariusze migracji bazy danych

W przypadku uaktualniania programu DPM 2012 R2 lub DPM 2016 do programu DPM 1801 przy użyciu:

1. Lokalne wystąpienie i migracja do zdalnego wystąpienia SQL Server podczas instalacji.
2. Wystąpienie zdalne i migracja do lokalnego wystąpienia SQL Server podczas instalacji.
3. Wystąpienie lokalne i migracja do zdalnego wystąpienia klastra SQL Server podczas instalacji.
4. Lokalne wystąpienie i migracja do innego lokalnego wystąpienia SQL Server podczas instalacji.
5. Zdalne wystąpienie i migracja do innego zdalnego wystąpienia SQL Server podczas instalacji.
6. Wystąpienie zdalne i migracja do zdalnego wystąpienia klastra SQL Server podczas instalacji.

Przygotowanie do migracji bazy danych

Jeśli chcesz użyć nowego programu SQL Server do migrowania DPM database, przed uaktualnieniem programu DPM upewnij się, że oba serwery SQL mają takie same:

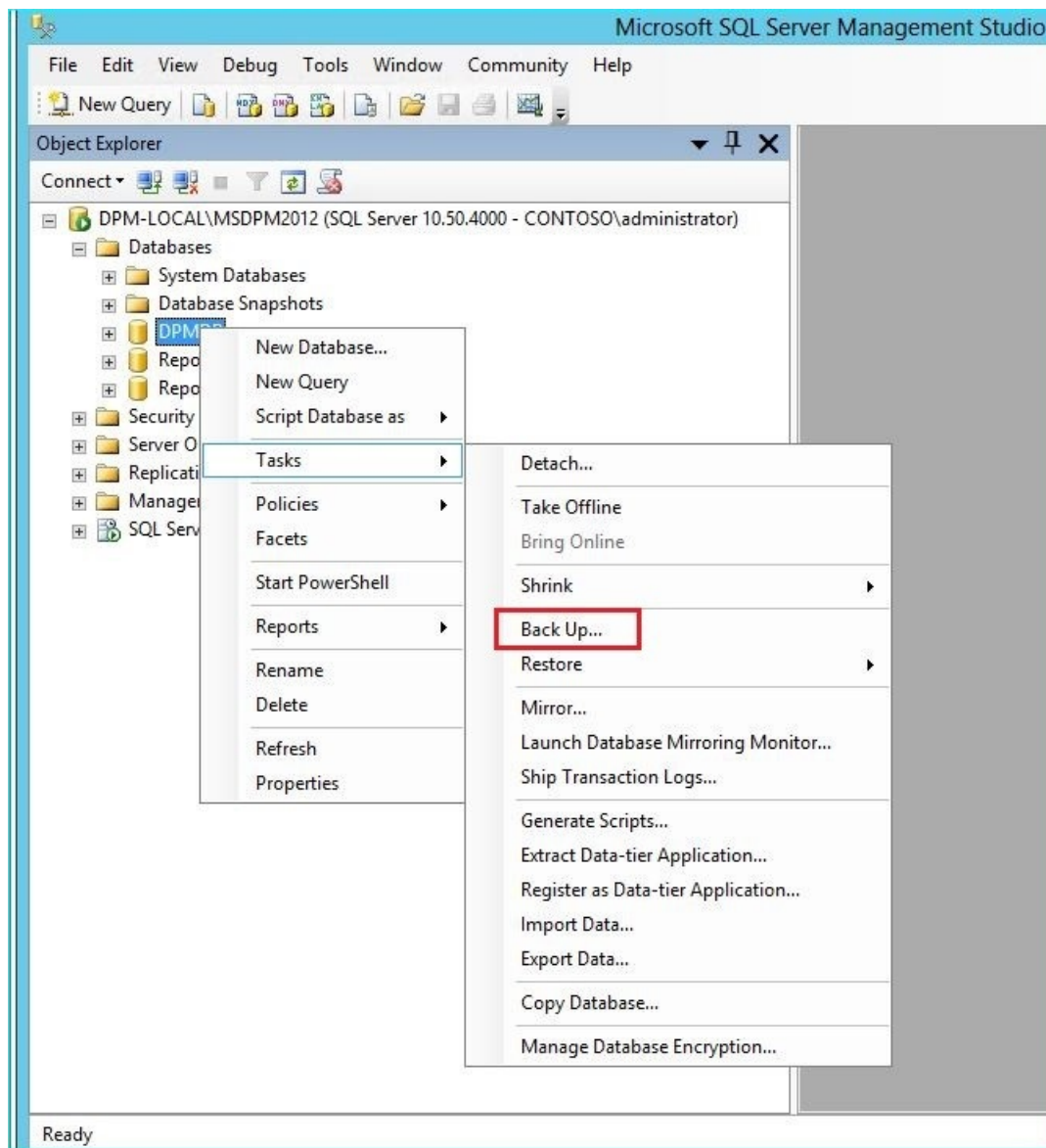
- Wymagania dotyczące programu SQL Server
- Konfiguracja konfiguracji
- Reguły zapory
- Pliki obsługi programu DPM ()

Gdy nowe wystąpienie SQL Server zainstalowane i przygotowane do użytku programu DPM, należy wykonać kopię zapasową bieżącego DPM database i przywrócić je na nowym SQL Server.

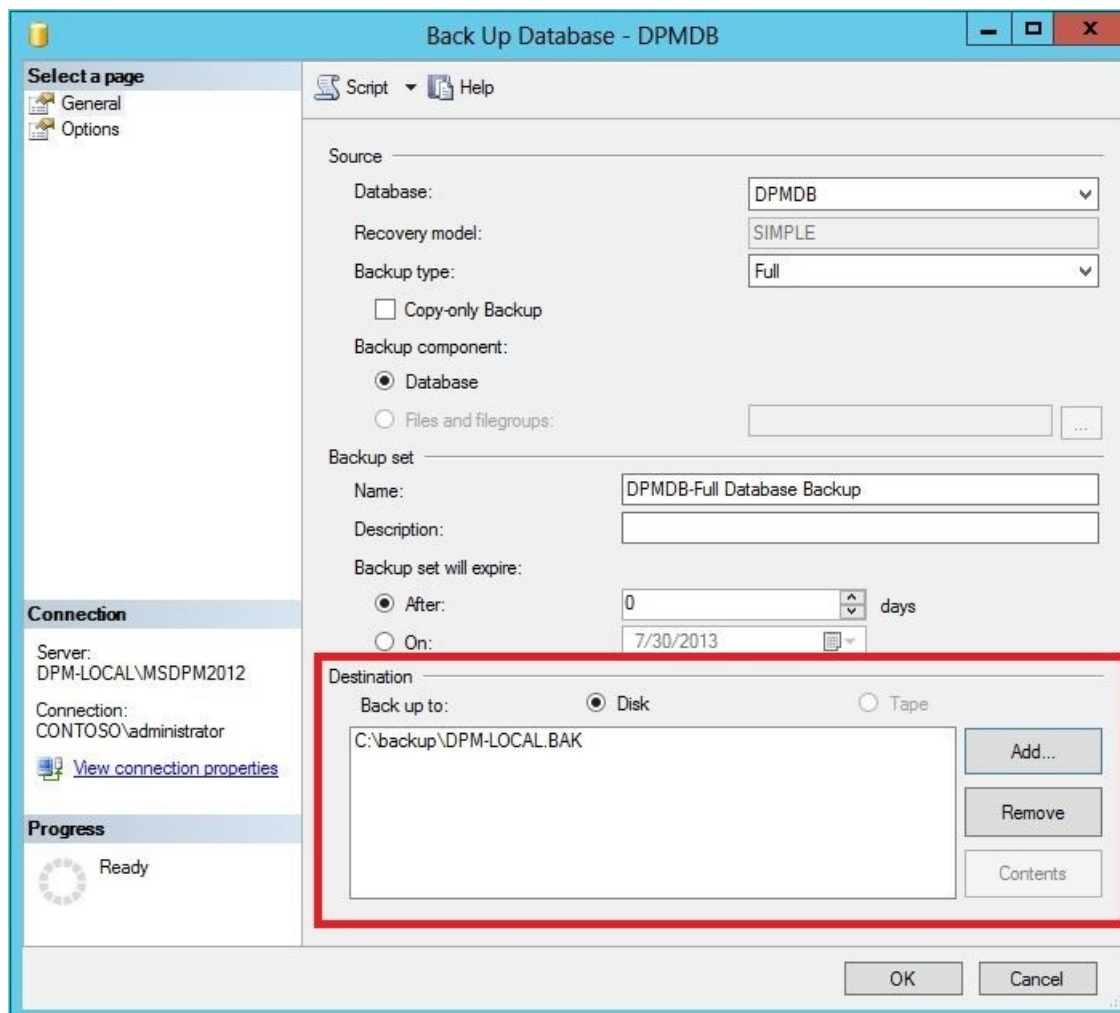
Kroki przed uaktualnieniem: utworzenie kopii zapasowej bazy danych DPM programu DPM 2012 R2 i przywrócenie jej w nowym wystąpieniu programu SQL

Ten przykład przygotowuje zdalny klaster SQL Server do użycia podczas migracji.

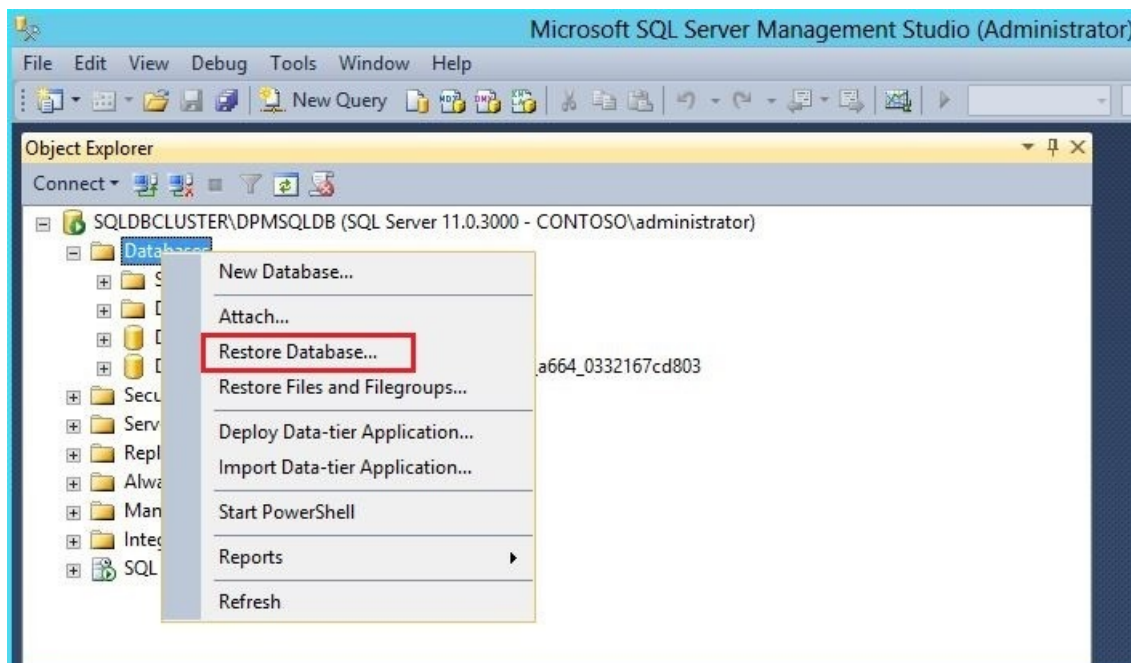
1. Na serwerze programu System Center Data Protection Manager 2012 R2 lub w zdalnym programie SQL Server hostującym bazę danych DPM uruchom program **Microsoft SQL Management Studio** i połącz się z wystąpieniem programu SQL hostującym bieżącą bazę danych DPMDB programu DPM 2012 R2.
2. Kliknij prawym przyciskiem myszy bazę danych DPM i w obszarze **Zadania** wybierz pozycję **Utwórz kopię zapasową...** .



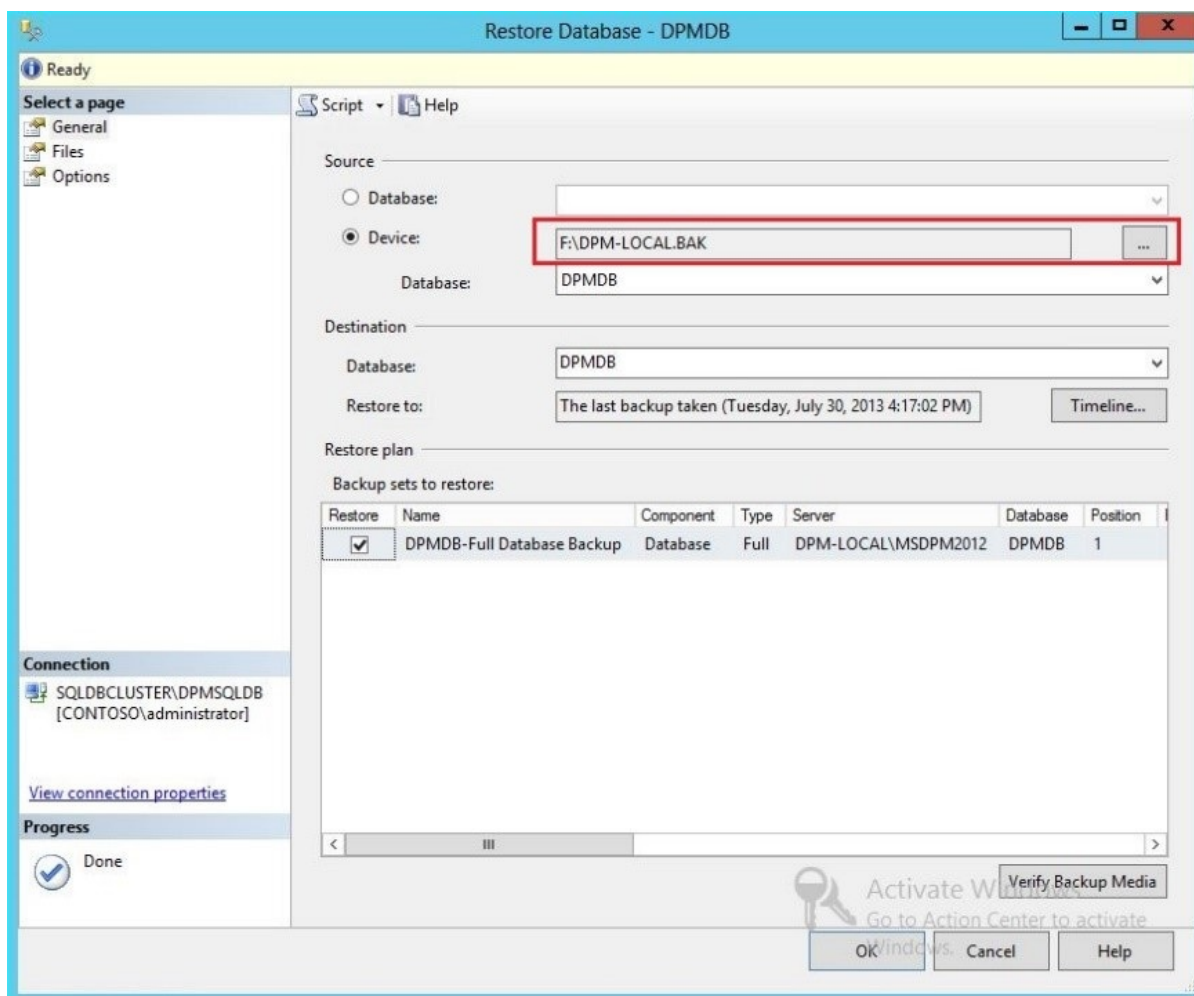
3. Dodaj miejsce docelowe kopii zapasowej i nazwę pliku, a następnie wybierz pozycję **OK**, aby rozpocząć tworzenie kopii zapasowej.



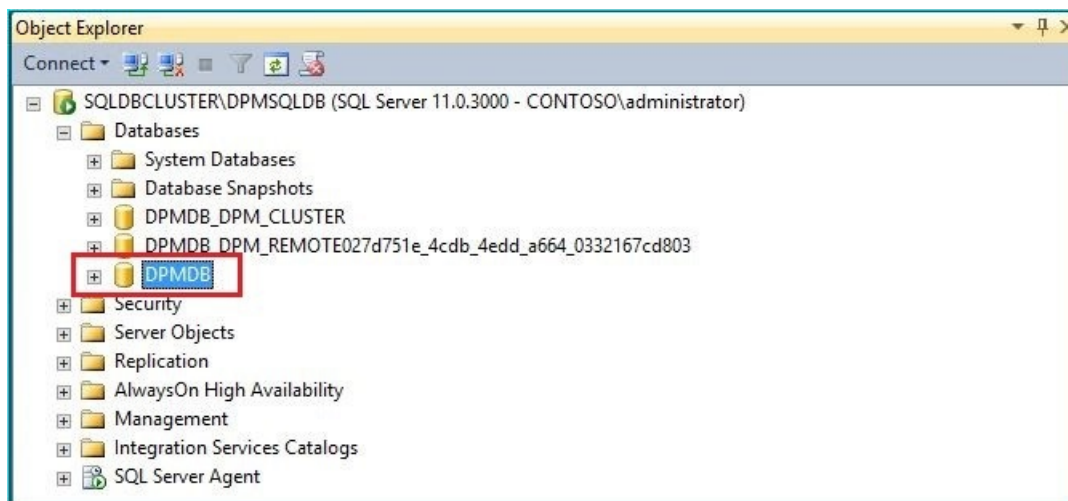
4. Po wykonaniu kopii zapasowej skopiuj plik wyjściowy do zdalnego programu SQL Server. Jeśli jest to klaster programu SQL, skopiuj go do aktywnego węzła hostującego wystąpienie programu SQL, którego chcesz użyć podczas uaktualniania programu DPM. Przed przystąpieniem do przywracania DPM database należy skopiować go na dysk udostępnionego klastra.
5. Na maszynie zdalnego programu SQL Server uruchom program **Microsoft SQL Management Studio** i połącz się z wystąpieniem programu SQL, którego chcesz użyć podczas uaktualniania programu DPM. Jeśli jest to klaster programu SQL, należy to zrobić w aktywnym węźle, do którego skopiowano plik kopii zapasowej. Plik kopii zapasowej teraz powinien znajdować się na udostępnionym dysku klastra.
6. Kliknij prawym przyciskiem myszy ikonę Bazy danych, a następnie wybierz polecenie **Przywróć bazę danych...** . Spowoduje to uruchomienie kreatora przywracania.



7. Wybierz pozycję **Urządzenie** w obszarze **Źródło**, a następnie znajdź plik kopii zapasowej bazy danych, który został skopiowany w poprzednim kroku, i wybierz go. Zweryfikuj opcje i lokalizację przywracania, a następnie wybierz pozycję **OK**, aby rozpocząć przywracanie. Rozwiąż wszelkie problemy zgłoszone podczas przywracania, aby zakończyć je pomyślnie.



8. Po zakończeniu przywracania przywrócona baza danych będzie widoczna w obszarze **Bazy danych** pod oryginalną nazwą. Ta baza danych zostanie użyta podczas uaktualniania. Możesz zakończyć program **Microsoft SQL Management Studio** i uruchomić proces uaktualniania na oryginalnym serwerze programu DPM.



9. Jeśli nowy program SQL Server jest zdalny, zainstaluj narzędzia zarządzania programem SQL na serwerze programu DPM. Wersja narzędzi zarządzania programem SQL musi pasować do wersji programu SQL Server hostującego bazę danych DPMDB.

Uruchomienie uaktualnienia w celu zmigrowania bazy danych DPMDB do innego programu SQL Server

NOTE

Jeśli wystąpienie programu SQL jest współużytkowane, uruchom instalację lub uaktualnienia programu DPM sekwencyjnie. Instalowanie równoległe może spowodować wystąpienie błędów.

1. Po zakończeniu kroków przygotowania przed migracją uruchom proces instalacji programu DPM 2016. Instalator programu DPM wyświetla informacje o bieżącym wystąpieniu programu SQL Server. W tym miejscu możesz wybrać inne wystąpienie programu SQL Server lub przejść na klastrowe wystąpienie programu SQL używane podczas migracji.

Data Protection Manager Setup

Prerequisites Check

Please wait while the wizard checks for required hardware and software.

Installation Stages

- Welcome
- Prerequisites check
- Product registration
- Installation settings
- Microsoft Update Opt-In
- Customer feedback option
- Installation

DPM requires a database. You can use a local or remote instance of SQL Server that already exists.

☒ Use stand-alone SQL Server.
SQL Server is not clustered.

☐ Use clustered SQL Server
SQL Server is clustered

Instance of SQL Server
(Example: SQLSERV or SQLSERV\MYSQLINSTANCE):

User Name: Password:

Domain:

Select the appropriate option and click on the button to perform the prerequisite check and install the missing Windows components.

< Back Next > Cancel Help

2. Zmień ustawienia programu SQL, aby użyć wystąpienia programu SQL Server, do którego przywrócono bazę danych DPM. Jeśli jest to klaster programu SQL, musisz także określić osobne wystąpienie programu SQL Server używane na potrzeby raportowania programu SQL. Przyjęto, że wszystkie reguły zapory oraz program SQLPrep zostały już uruchomione. Musisz podać poprawne poświadczenia, a następnie kliknąć przycisk **Sprawdź i instaluj**.

Data Protection Manager Setup

Prerequisites Check

Please wait while the wizard checks for required hardware and software.

Installation Stages

- Welcome
- Prerequisites check**
- Product registration
- Installation settings
- Microsoft Update Opt-In
- Customer feedback option
- Installation

DPM requires a database. You can use a local or remote instance of SQL Server that already exists.

☐ Use stand-alone SQL Server.
 SQL Server is not clustered.

☒ Use clustered SQL Server
 SQL Server is clustered

Instance of SQL Server
(Example: SQLSERV or SQLSERV\MYSQLINSTANCE):

SQLDBCLUSTER\DPMSQLDB

User Name: Administrator Password: *****

Domain: contoso

Instance of SQL Server Reporting Service
(Example: SQLSERV or SQLSERV\MYREPORTINGINSTANCE):

SQLSERVER\DPMSQLDB

User Name: Administrator Password: *****

Domain: contoso

Select the appropriate option and click on the button to perform the prerequisite check and install the missing Windows components.

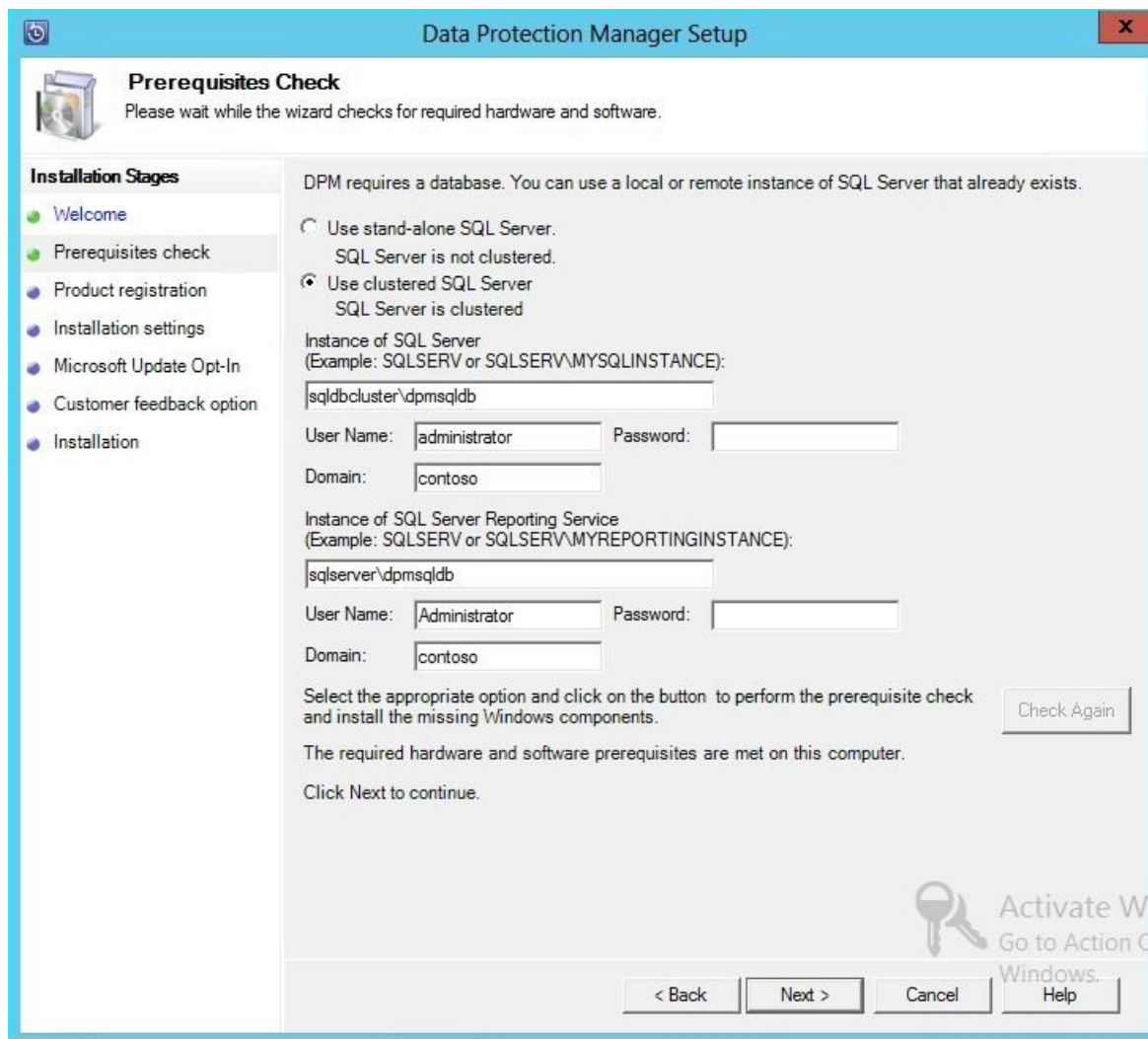
Check and Install

Details

Setup will use the current user's credentials for this SQL instance.

< Back Next > Cancel Help

3. Sprawdzanie wymagań wstępnych powinno zakończyć się pomyślnie. Naciśnij pozycję DALEJ, aby kontynuować uaktualnianie.



4. Kontynuuj pracę kreatora.
5. Po zakończeniu instalacji odpowiadająca baza danych w ramach określonego wystąpienia będzie miała teraz nazwę DPMPB_DPMNazwaSerwera. Ponieważ może być ona współużytkowana z innymi serwerami programu DPM, konwencja nazewnictwa dla bazy danych DPM będzie teraz następująca:
DPM2016\$DPMDB_DPMNazwaSerwera

Dodawanie miejsca do magazynowania dla funkcji Modern Backup Storage

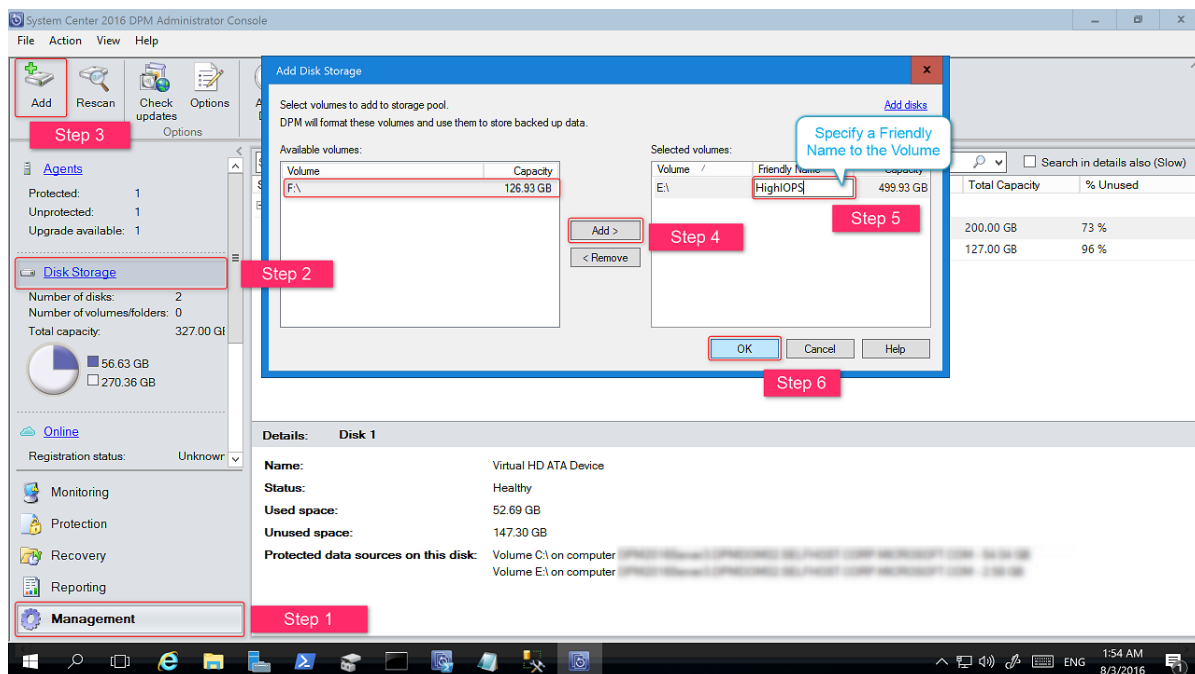
Aby wydajnie przechowywać kopie zapasowe, program DPM 2016 używa woluminów. Można także kontynuować przechowywanie kopii zapasowych na dyskach, jak w programie DPM 2012 R2.

Dodawanie woluminów i dysków

Jeśli uruchamiasz program DPM 2016 w systemie Windows Server, możesz przechowywać dane kopii zapasowych na woluminach. Woluminy pozwalają zaoszczędzić miejsce do magazynowania i zapewniają szybsze tworzenie kopii zapasowych. Możesz nadać woluminowi przyjazną nazwę i możesz zmienić jego nazwę. Podaj przyjazną nazwę podczas dodawania woluminu lub później, klikając kolumnę **Przyjazna nazwa** wybranego woluminu. Za pomocą programu PowerShell także można dodawać i zmieniać przyjazne nazwy dla woluminów.

Aby dodać wolumin w konsoli administratora:

1. W konsoli administratora programu DPM wybierz funkcję **Zarządzanie**, a następnie wybierz pozycję **Magazyn dyskowy > Dodaj**.
2. W oknie dialogowym **dodawanie Disk Storage** wybierz dostępny wolumin > kliknij przycisk **Dodaj** > Wpisz przyjazną nazwę woluminu > kliknij przycisk **OK**.



Jeśli chcesz dodać dysk, musi on należeć do grupy ochrony ze starszą wersją magazynu. Te dyski mogą być używane tylko dla tych grup ochrony. Jeśli serwer programu DPM nie ma źródła ze starszą ochroną, dysk nie będzie widoczny. Aby uzyskać więcej informacji na temat dodawania dysków, zobacz [Dodawanie dysków w celu zwiększenia miejsca w starszej wersji magazynu](#). Dyskowi nie można nadać przyjaznej nazwy.

Przypisywanie obciążeń do woluminów

Program DPM 2016 umożliwia użytkownikowi określenie, jakie rodzaje obciążeń powinny być przypisane do poszczególnych woluminów. Na przykład kosztowne woluminy, które obsługują bardzo duże liczby operacji we/wy na sekundę, można skonfigurować tak, aby przechowywały tylko obciążenia wymagające częstego tworzenia dużych kopii zapasowych, jak w przypadku programu SQL z dziennikami transakcji. Aby zaktualizować właściwości woluminu w puli magazynów na serwerze programu DPM, użyj polecenia cmdlet programu PowerShell: Update-DPMDiskStorage.

Update-DPMDiskStorage

Składnia

Parameter Set: Volume

```
Update-DPMDiskStorage [-Volume] <Volume> [[-FriendlyName] <String> ] [[-DatasourceType] <VolumeTag[]> ] [-Confirm] [-WhatIf] [ <CommonParameters>]
```

Zmiany wprowadzone za pomocą programu PowerShell są odzwierciedlane w interfejsie użytkownika.

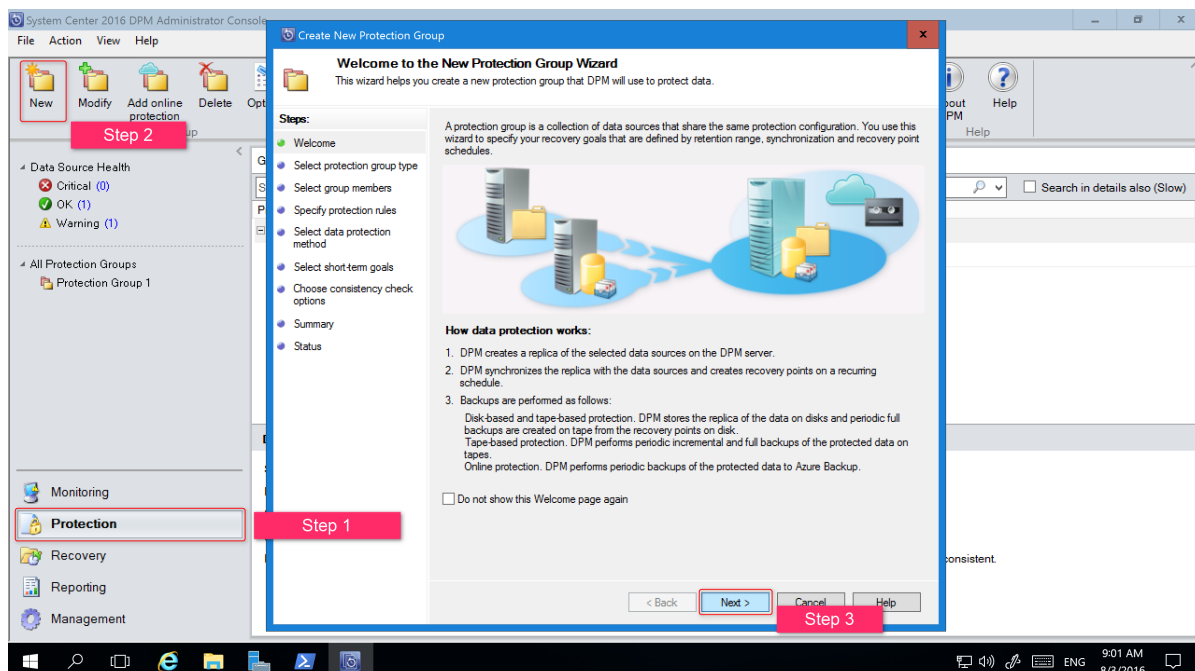
Ochrona źródeł danych

Aby rozpocząć ochronę źródeł danych, utwórz grupę ochrony. Poniższa procedura podkreśla zmiany i dodatki w kreatorze **Nowa grupa ochrony**.

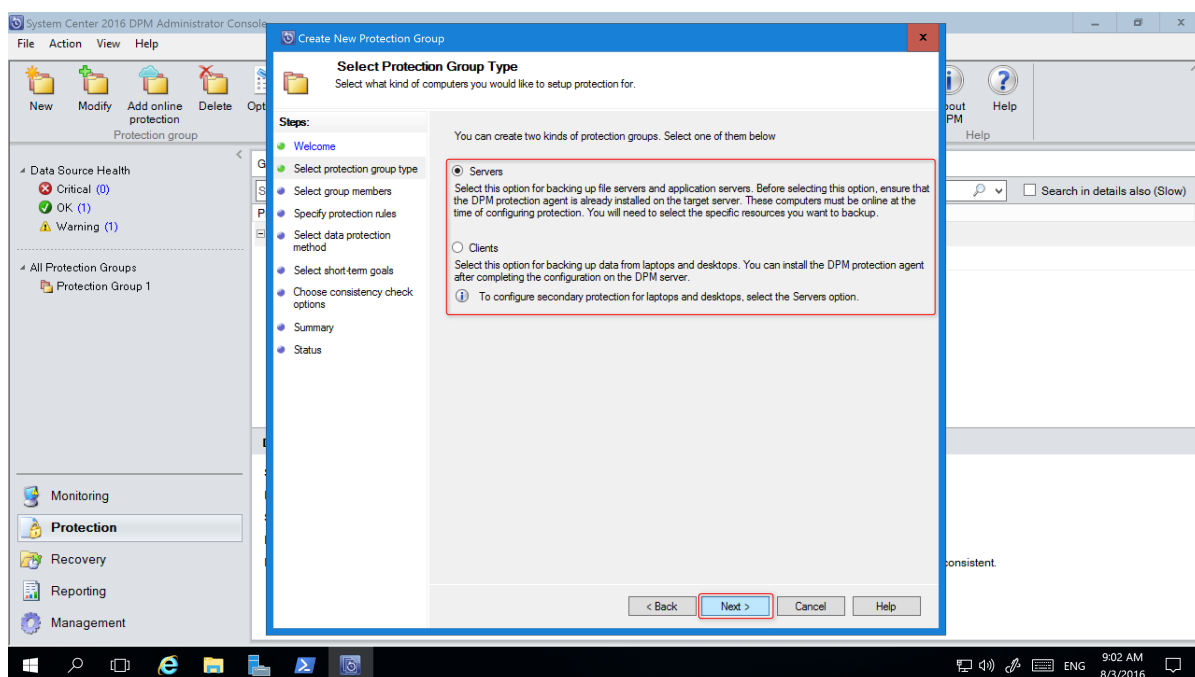
Aby utworzyć grupę ochrony:

1. W konsoli administratora programu DPM wybierz funkcję **Ochrona**.
2. Na wstążce narzędzi kliknij pozycję **Nowy**.

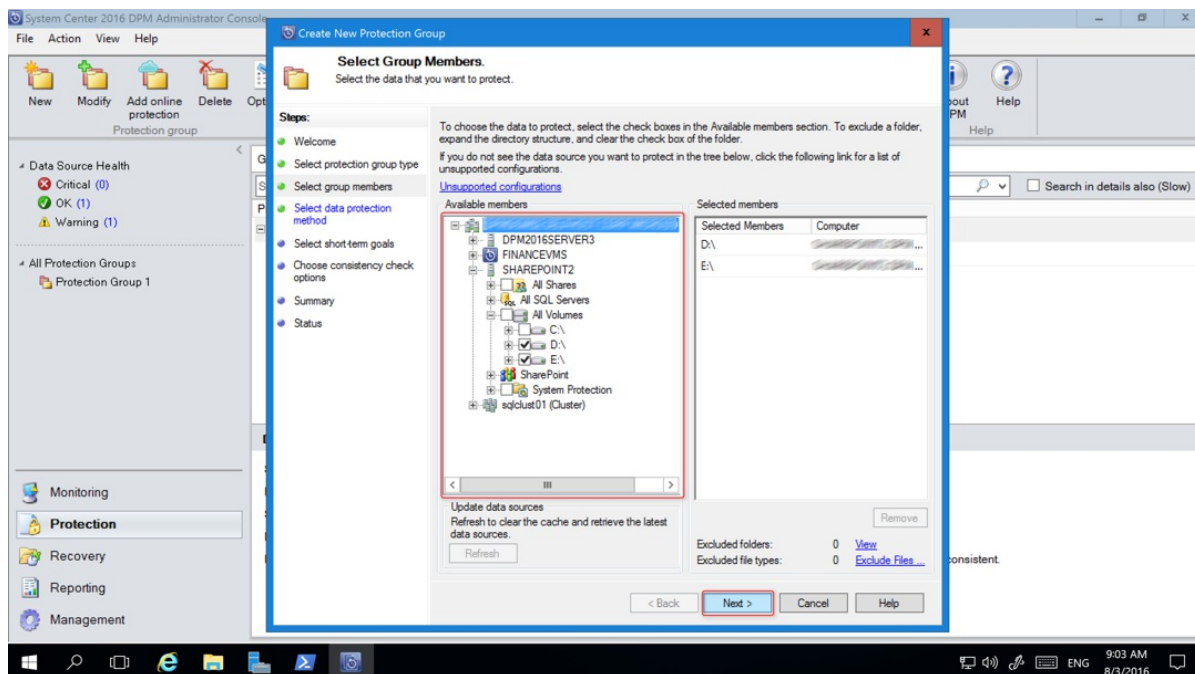
Zostanie otwarty kreator **Utwórz nową grupę ochrony**.



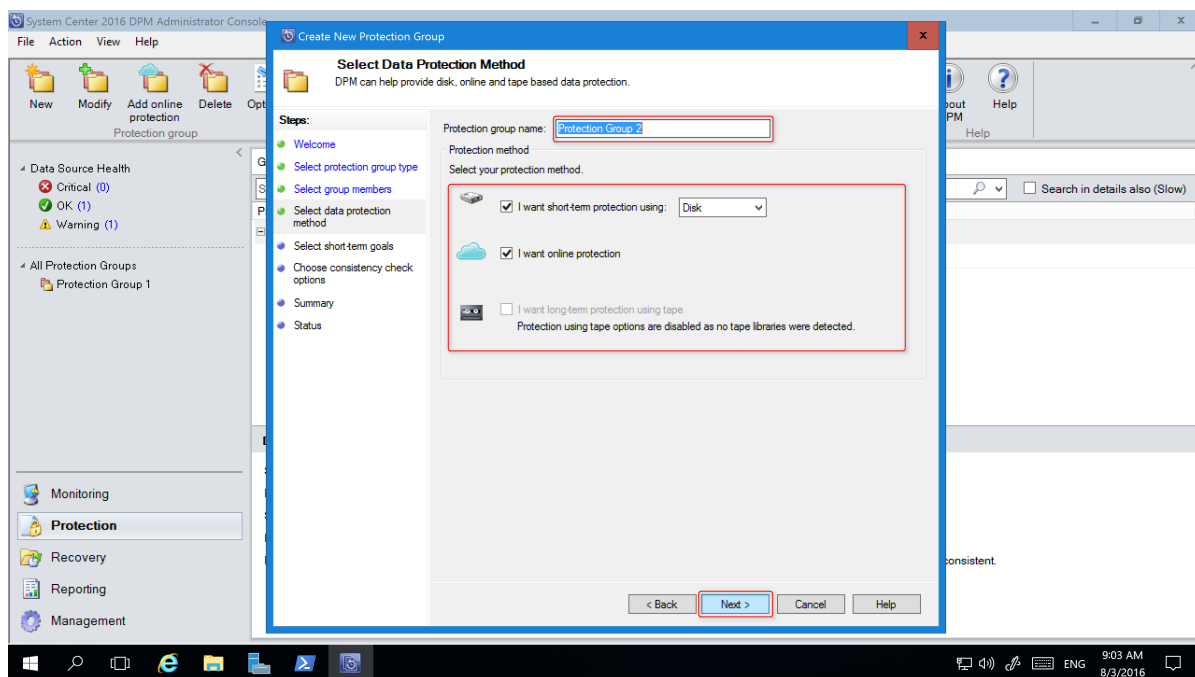
3. Kliknij przycisk **Dalej**, aby przejść w kreatorze do ekranu **Wybierz typ grupy ochrony**.
4. Na ekranie **Wybierz typ grupy ochrony** wybierz typ grupy ochrony, który ma zostać utworzony, a następnie kliknij przycisk **Dalej**.



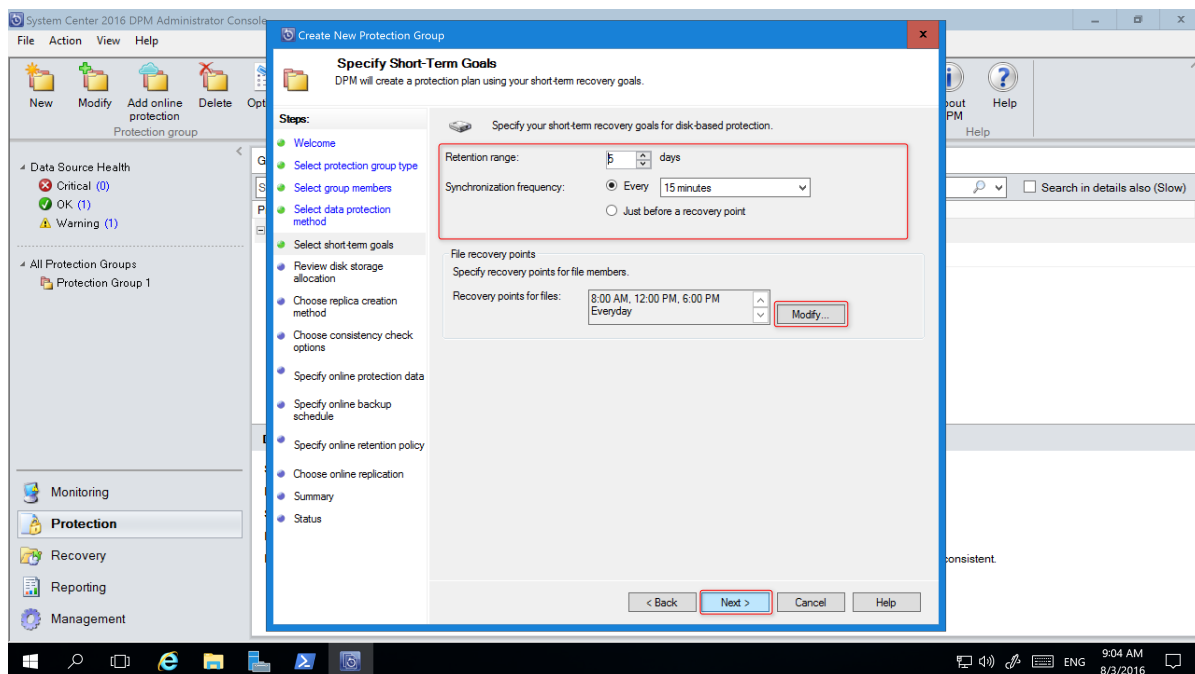
5. Na ekranie **Wybierz elementy członkowskie grupy** w okienku **Dostępne elementy członkowskie** program DPM wyświetla listę elementów członkowskich z agentami ochrony. Na potrzeby tego przykładu wybierz woluminy D:\ i E:, aby dodać je do okienka **Wybrane elementy członkowskie**. Po wybraniu elementów członkowskich do grupy ochrony kliknij przycisk **Dalej**.



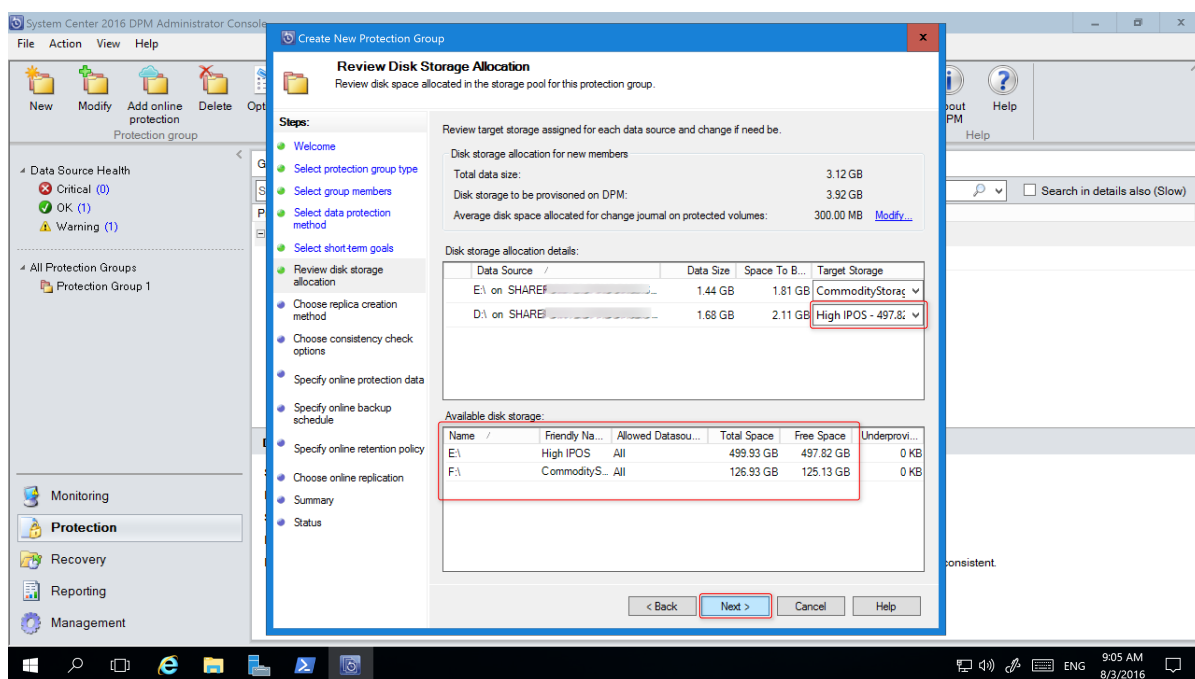
6. Na ekranie **Wybierz metodę ochrony danych** w polu **Grupa ochrony** wpisz nazwę grupy ochrony, wybierz metody ochrony i kliknij przycisk **Dalej**. Jeśli chcesz ochrony krótkoterminowej, musisz użyć kopii zapasowej dysku.



7. Na ekranie **Określ cele krótkoterminowe** określ szczegóły w polach **Zakres przechowywania** i **Częstotliwość synchronizacji**, a następnie kliknij przycisk **Dalej**. Jeśli chcesz, kliknij przycisk **Modyfikuj**, aby zmienić harmonogram wykonywania punktów odzyskiwania.

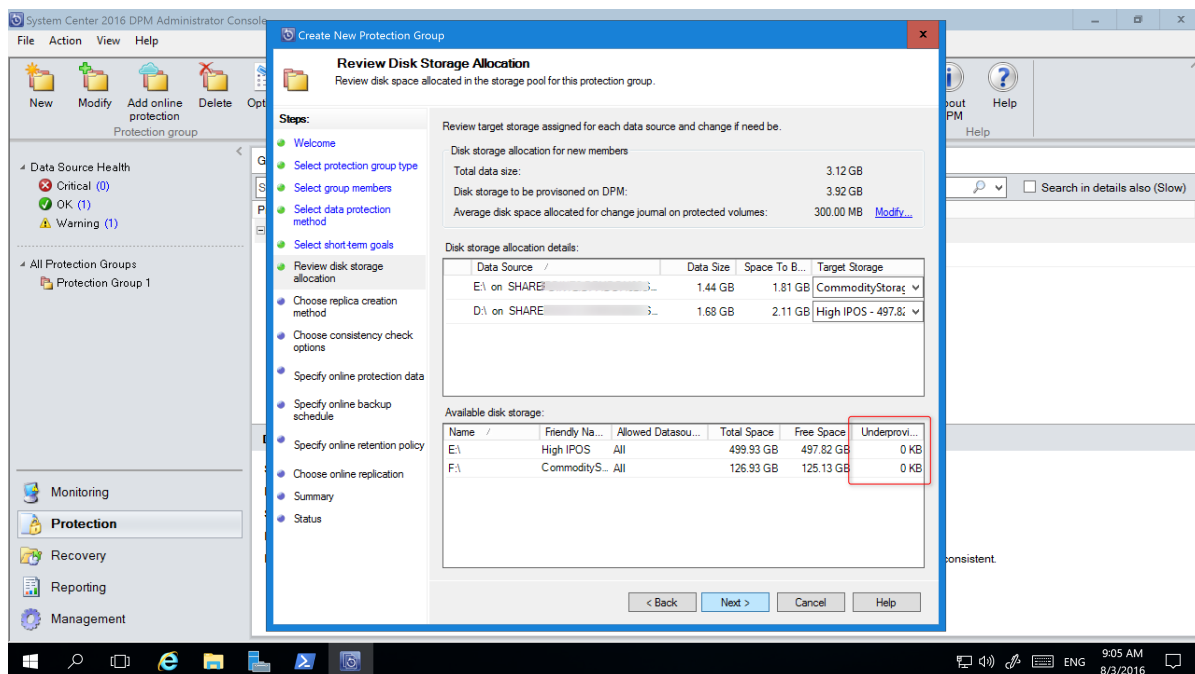


8. Ekran **Przejrzyj przydział magazynu dyskowego** zawiera szczegółowe informacje dotyczące wybranych źródeł danych i ich wielkości oraz dane w obszarach **Miejsce na potrzeby aprowizacji** i **Docelowy wolumin magazynu**.



Woluminy magazynu są określane na podstawie alokacji woluminu obciążenia (ustawianego przy użyciu programu PowerShell) i dostępnego miejsca do magazynowania. Woluminy magazynu można zmienić, wybierając inne woluminy z menu rozwijanego. Jeśli zmienisz wartość w polu **Magazyn docelowy**, dane w polu **Dostępny magazyn dyskowy** zmieniają się dynamicznie, aby odzwierciedlić wartości w polach **Wolne miejsce** i **Miejsce poniżej aprowizacji**.

Kolumna **Miejsce poniżej aprowizacji** w obszarze **Dostępny magazyn dyskowy** odzwierciedla ilość dodatkowego miejsca, które będzie potrzebne, jeśli źródła danych zwiększą się zgodnie z planem. Użyj tej wartości, aby pomóc w zaplanowaniu potrzeb magazynowych w celu umożliwienia bezproblemowego tworzenia kopii zapasowych. Jeśli ta wartość wynosi zero, oznacza to, że w najbliższej przyszłości nie ma potencjalnych problemów z magazynem. Jeśli wartość jest różna od zera, oznacza to, że przydzielone miejsce w magazynie nie jest wystarczające — na podstawie zasad ochrony i rozmiaru danych chronionych elementów członkowskich.

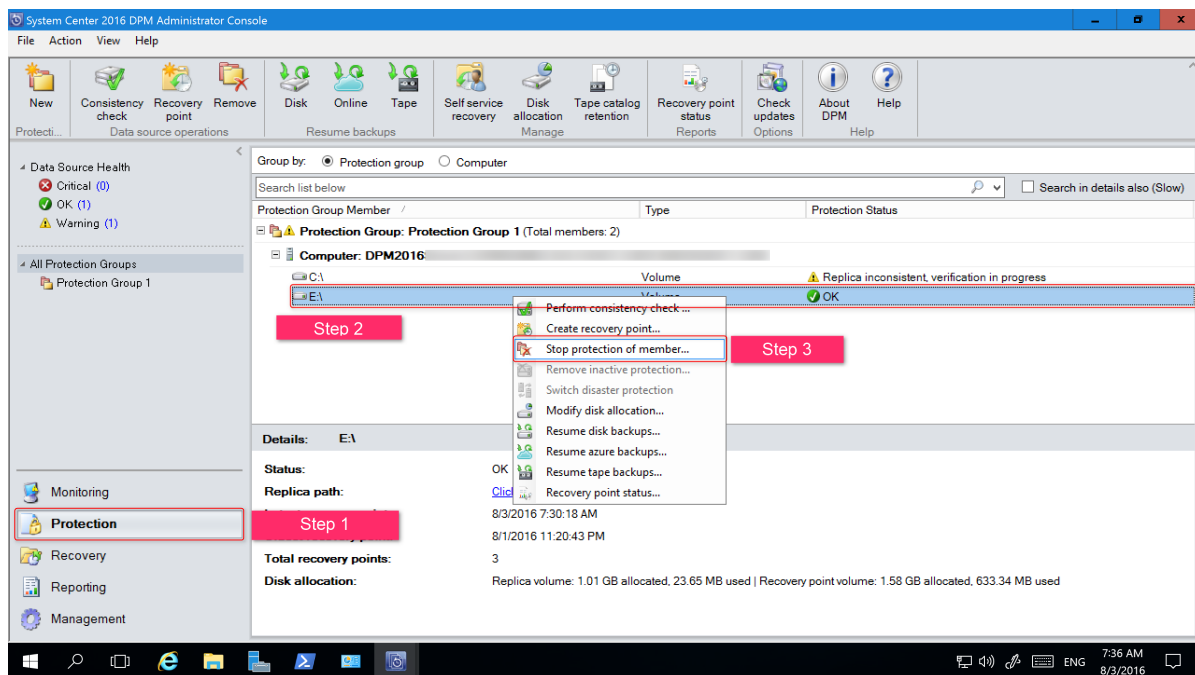


Pozostała część Kreatora nowej grupy ochrony jest taka sama, jak w programie DPM 2012 R2. Kontynuuj wykonywanie kroków kreatora, aby ukończyć tworzenie nowej grupy ochrony.

Migrowanie starszej wersji magazynu do funkcji Modern Backup Storage

Po uaktualnieniu programu DPM 2012 R2 do programu DPM 2016 i systemu operacyjnego do wersji Windows Server 2016 można zaktualizować istniejące grupy ochrony do nowych funkcji programu DPM 2016. Domyślnie grupy ochrony nie są zmieniane i nadal funkcjonują tak, jak zostały skonfigurowane w programie DPM 2012 R2. Aktualizowanie grup ochrony w celu korzystania z funkcji Modern Backup Storage jest opcjonalne. Aby zaktualizować grupę ochrony, zatrzymaj ochronę wszystkich źródeł danych z opcją zachowania danych, a następnie dodaj źródła danych do nowej grupy ochrony. Program DPM zacznie chronić te źródła danych w nowy sposób.

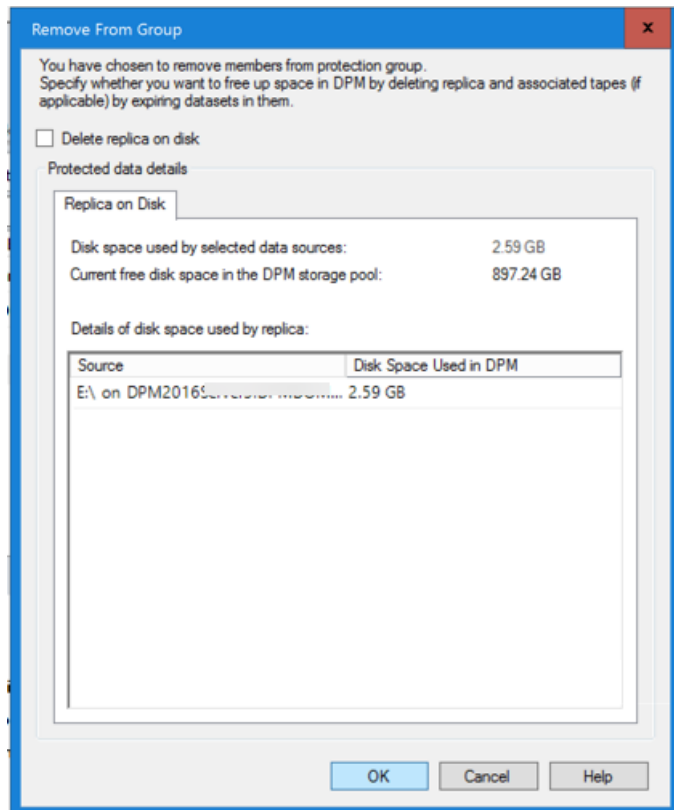
1. W konsoli administratora wybierz funkcję **Ochrona** i na liście **Element członkowski grupy ochrony** kliknij prawym przyciskiem myszy wybrany element członkowski, a następnie wybierz polecenie **Zatrzymaj ochronę elementu członkowskiego**.



Zostanie otwarte okno dialogowe **Usuń z grupy**.

2. W oknie dialogowym **Usuń z grupy** przejrzyj używane miejsce na dysku i dostępne wolne miejsce w puli magazynów. Domyślnie punkty odzyskiwania pozostają na dysku i wygasają zgodnie ze skojarzonymi z nimi zasadami przechowywania. Kliknij przycisk **OK**.

Aby natychmiast przywrócić zajęte miejsce na dysku do wolnej puli magazynów, zaznacz opcję **Usuń replikę z dysku**. Spowoduje to usunięcie danych kopii zapasowej (i punktów odzyskiwania) skojarzonych z tym elementem członkowskim.



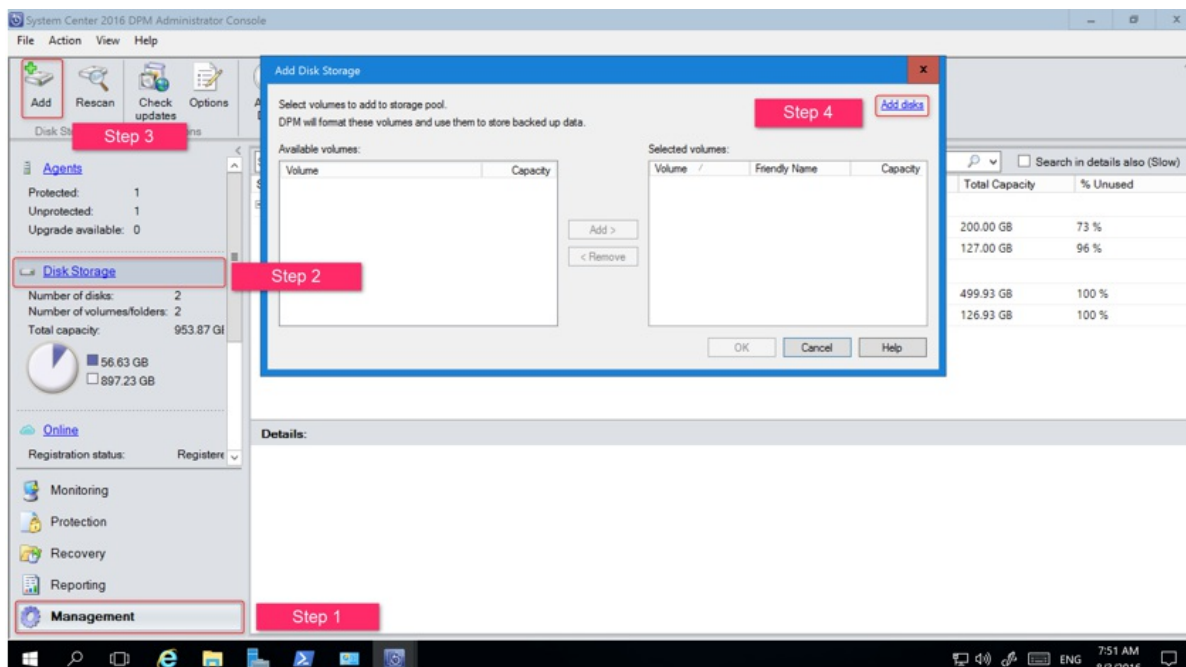
3. Utwórz nową grupę ochrony, która używa Nowoczesny magazyn kopii zapasowych i Uwzględnij niechronione źródła danych.

Dodawanie dysków w celu zwiększenia magazynu w starszej wersji

Jeśli chcesz używać starszej wersji magazynu z programem DPM 2016, może być konieczne dodanie dysków w celu zwiększenia magazynu w starszej wersji. Aby dodać magazyn dyskowy:

1. W konsoli administratora kliknij pozycję **Zarządzanie**.
2. Wybierz pozycję **Magazyn dyskowy**.
3. Na wstążce narzędzi kliknij pozycję **Nowy**.

Zostanie otwarte okno dialogowe **Dodawanie magazynu dyskowego**.



4. W oknie dialogowym **Dodawanie magazynu dyskowego** kliknij pozycję **Dodaj dyski**.

Program DPM wyświetli listę dostępnych dysków.

5. Wybierz dyski, kliknij przycisk **Dodaj**, aby dodać te dyski, a następnie kliknij przycisk **OK**.

Nowe polecenia cmdlet programu PowerShell

W programie DPM 2016 dostępne są dwa nowe polecenia cmdlet: [Mount-DPMRecoveryPoint](#) i [Dismount-DPMRecoveryPoint](#). Kliknij nazwę polecenia cmdlet, aby wyświetlić dotyczącą go dokumentację.

Włączanie ochrony w chmurze

Kopię zapasową serwera programu DPM można utworzyć na platformie Azure. Ogólna procedura jest następująca:

- Utwórz subskrypcję platformy Azure.
- Zarejestruj serwer w usłudze Kopia zapasowa Azure.
- Pobierz poświadczenia magazynu i agenta kopii zapasowej Azure.
- Skonfiguruj poświadczenia magazynu i zasady tworzenia kopii zapasowej serwera.

Aby uzyskać więcej informacji na temat tworzenia kopii zapasowych programu DPM w chmurze, zapoznaj się z artykułem [przygotowanie do tworzenia kopii zapasowych obciążeń na platformie Azure przy użyciu programu DPM](#).

Ten artykuł zawiera informacje o uaktualnianiu programu System Center 2016 — Data Protection Manager (DPM).

Uaktualnianie do programu DPM 2016

Program DPM 2016 możesz zainstalować w systemie Windows Server 2012 R2 lub Windows Server 2016. Jeśli instalujesz program DPM 2016 w systemie Windows Server 2012 R2, musisz uaktualnić istniejącą instalację programu DPM w wersji DPM 2012 R2 z pakietem zbiorczym aktualizacji 10 lub nowszym. Zanim uaktualnisz lub zainstalujesz program DPM 2016, przeczytaj temat [Wymagania wstępne instalacji](#).

Ścieżka uaktualnienia dla programu DPM 2016

Jeśli zamierzasz uaktualnić poprzednią wersję programu DPM do wersji DPM 2016, upewnij się, że Twoja instalacja zawiera niezbędne aktualizacje:

- Uaktualnij program DPM 2012 R2 do programu DPM 2012 R2 z pakietem zbiorczym aktualizacji 10. Pakiety zbiorcze aktualizacji można uzyskać z usługi Windows Update.
- Uaktualnij program DPM 2012 R2 z pakietem zbiorczym aktualizacji 10 do programu DPM 2016.
- Zaktualizuj agentów na serwerach chronionych.
- Uaktualnij system Windows Server 2012 R2 do systemu Windows Server 2016.
- Uaktualnij usługę Administracja zdalna programu DPM na wszystkich serwerach produkcyjnych.
- Tworzenie kopii zapasowych będzie kontynuowane bez ponownego rozruchu serwera produkcyjnego.

Procedura uaktualniania programu DPM

1. Aby zainstalować program DPM, kliknij dwukrotnie plik Setup.exe w celu otworzenia Kreatora programu System Center 2016.
2. W obszarze Zainstaluj kliknij pozycję Data Protection Manager. Spowoduje to uruchomienie Instalatora. Zaakceptuj warunki i postanowienia licencyjne, a następnie wykonaj kroki Kreatora instalacji.

Niektóre funkcje programu DPM 2016, takie jak Modern Backup Storage, wymagają kompilacji Windows Server 2016 RTM. Można uaktualnić program DPM 2012 R2 do programu DPM 2016 w systemie Windows Server 2012 R2. Jednak klienci otrzymujący program DPM 2016 będą chcieli korzystać z najnowszych funkcji, dlatego firma Microsoft zaleca instalowanie programu DPM 2016 na nowej instalacji systemu Windows Server 2016 RTM. Instrukcje dotyczące instalowania programu DPM można znaleźć w artykule [Instalowanie programu DPM 2016](#).

Migrowanie bazy danych DPM podczas uaktualniania

W ramach uaktualniania możesz przenieść bazę danych DPM. Na przykład w przypadku scalania wystąpień programu SQL Server. Jeśli wykonujesz przeniesienie do zdalnego programu SQL Server o wyższej wydajności. Jeśli chcesz dodać odporność na uszkodzenia za pomocą klastra programu SQL Server lub wykonać przeniesienie między zdalnym i lokalnym programem SQL Server w dowolną stronę. Instalator programu DPM 2016 umożliwia migrację bazy danych DPM do innych programów SQL Server podczas uaktualniania.

Możliwe scenariusze migracji bazy danych

1. Uaktualnienie programu DPM 2012 R2 przy użyciu lokalnego wystąpienia i migracja do zdalnego wystąpienia programu SQL Server podczas instalacji.
2. Uaktualnienie programu DPM 2012 R2 przy użyciu zdalnego wystąpienia i migracja do lokalnego wystąpienia programu SQL Server podczas instalacji.
3. Uaktualnienie programu DPM 2012 R2 przy użyciu lokalnego wystąpienia i migracja do zdalnego wystąpienia klastra programu SQL Server podczas instalacji.
4. Uaktualnienie programu DPM 2012 R2 przy użyciu lokalnego wystąpienia i migracja do innego lokalnego wystąpienia programu SQL Server podczas instalacji.
5. Uaktualnienie programu DPM 2012 R2 przy użyciu zdalnego wystąpienia i migracja do innego zdalnego wystąpienia programu SQL Server podczas instalacji.
6. Uaktualnienie programu DPM 2012 R2 przy użyciu zdalnego wystąpienia i migracja do zdalnego wystąpienia klastra programu SQL Server podczas instalacji.

Przygotowanie do migracji bazy danych

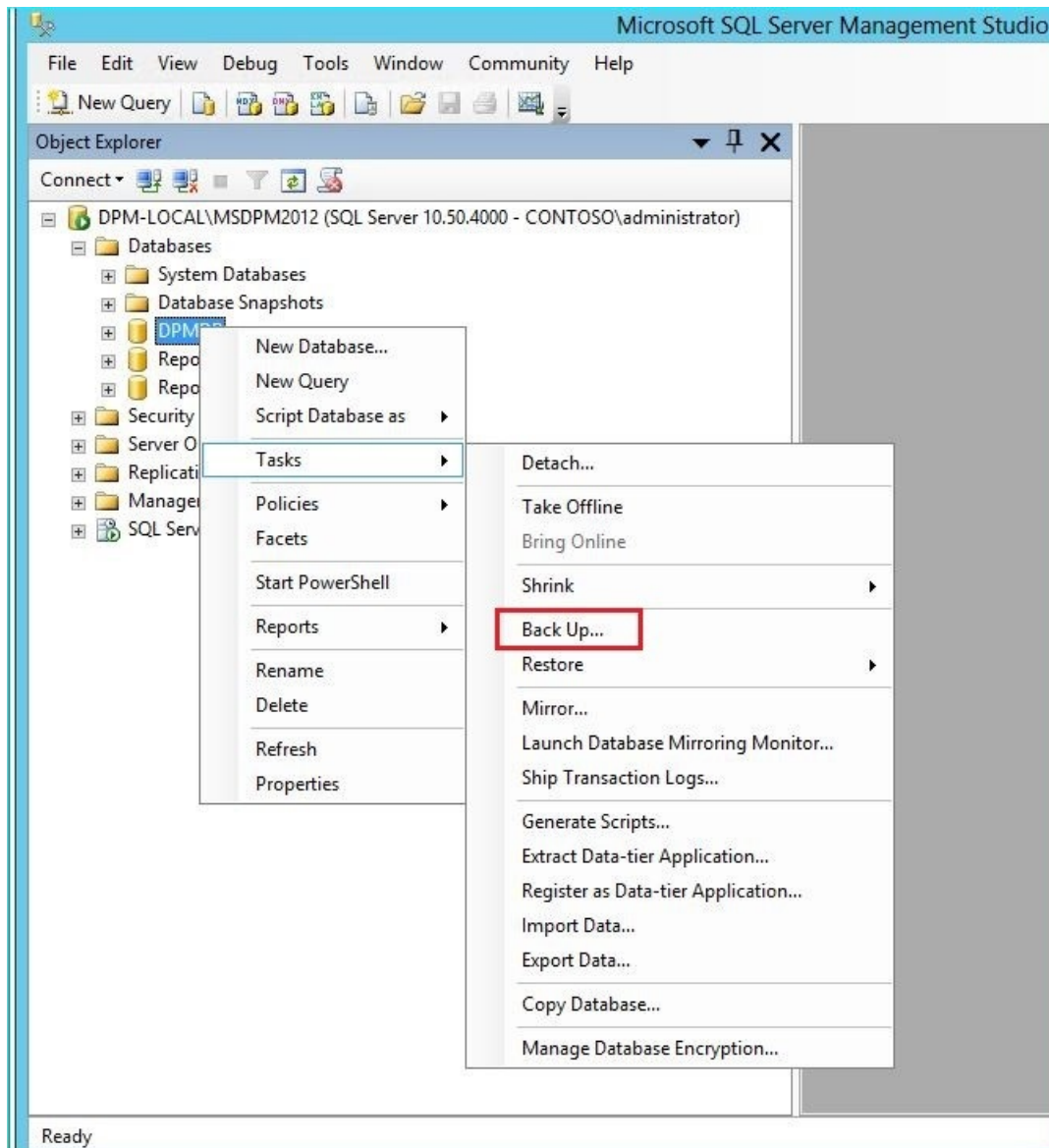
Nowy program SQL Server, którego chcesz użyć do migracji bazy danych DPM, musi spełniać takie same wymagania programu SQL Server oraz mieć taką samą konfigurację instalacji, reguły zapory i zainstalowane pliki obsługi programu DPM (sqlprep) przed wykonaniem uaktualnienia programu DPM.

Po zainstalowaniu nowego wystąpienia programu SQL Server i jego przygotowaniu pod kątem programu DPM należy wykonać kopię zapasową bieżącej bazy danych programu DPM 2012 R2 UR10 KB3143871 (4.2.1473.0) lub nowszego i przywrócić ją w nowym programie SQL Server.

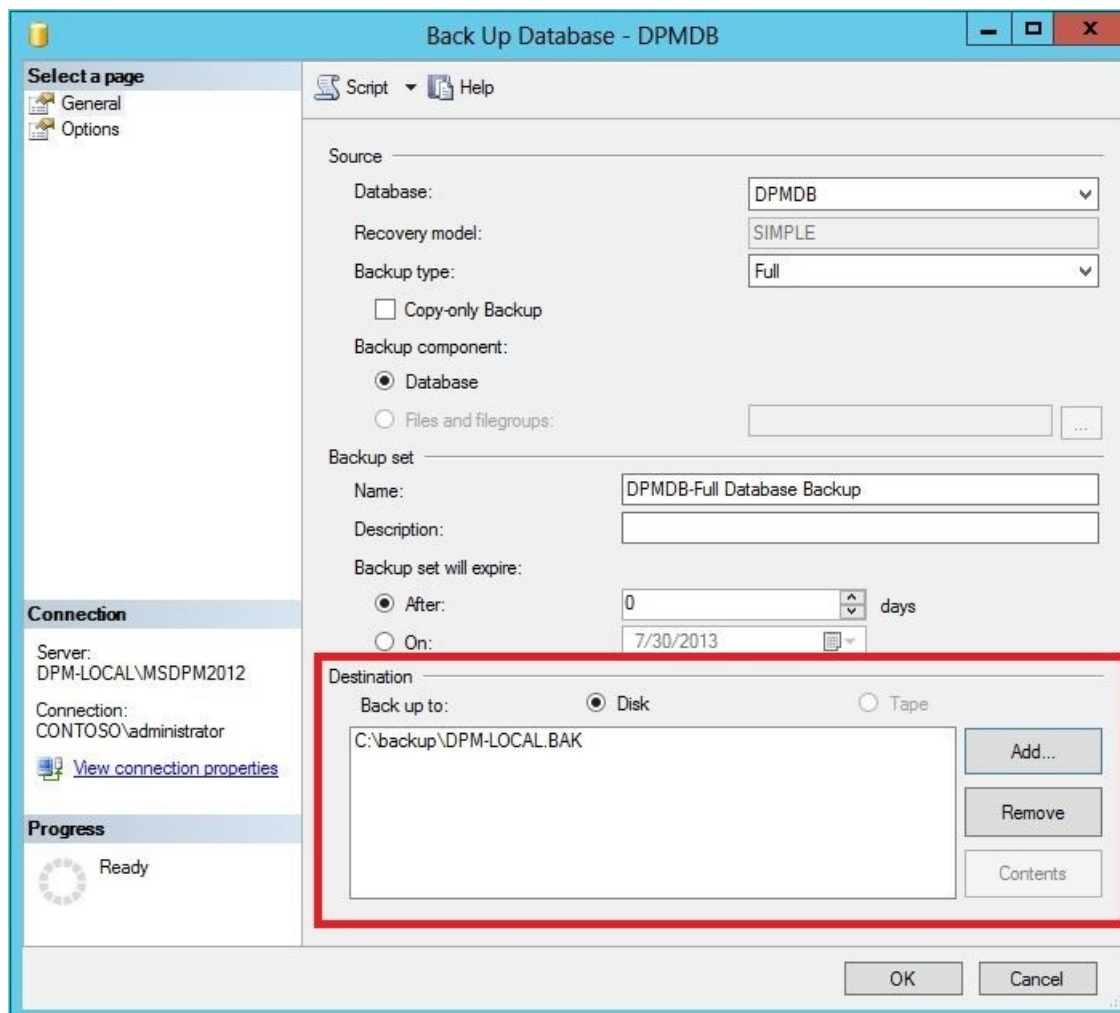
Kroki przed uaktualnieniem: utworzenie kopii zapasowej bazy danych DPM programu DPM 2012 R2 i przywrócenie jej w nowym wystąpieniu programu SQL

W ramach tego przykładu zostanie przygotowany zdalny klaster programu SQL Server na potrzeby migracji.

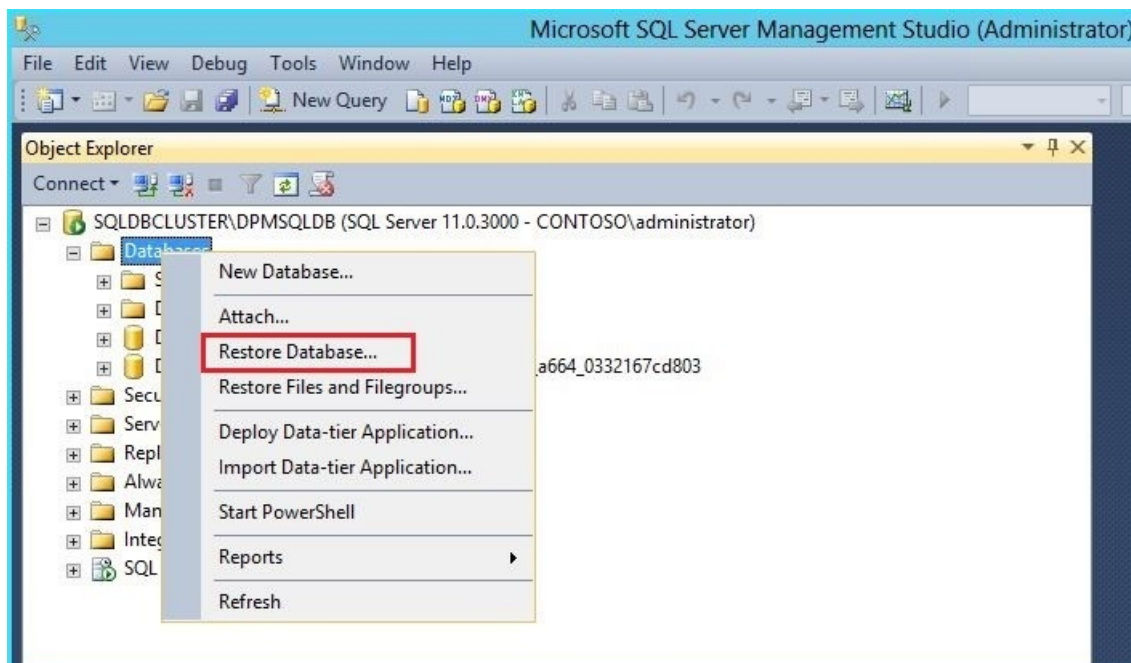
1. Na serwerze programu System Center Data Protection Manager 2012 R2 lub w zdalnym programie SQL Server hostującym bazę danych DPM uruchom program **Microsoft SQL Management Studio** i połącz się z wystąpieniem programu SQL hostującym bieżącą bazę danych DPMDb programu DPM 2012 R2.
2. Kliknij prawym przyciskiem myszy bazę danych DPM i w obszarze **Zadania** wybierz pozycję **Utwórz kopię zapasową...**.



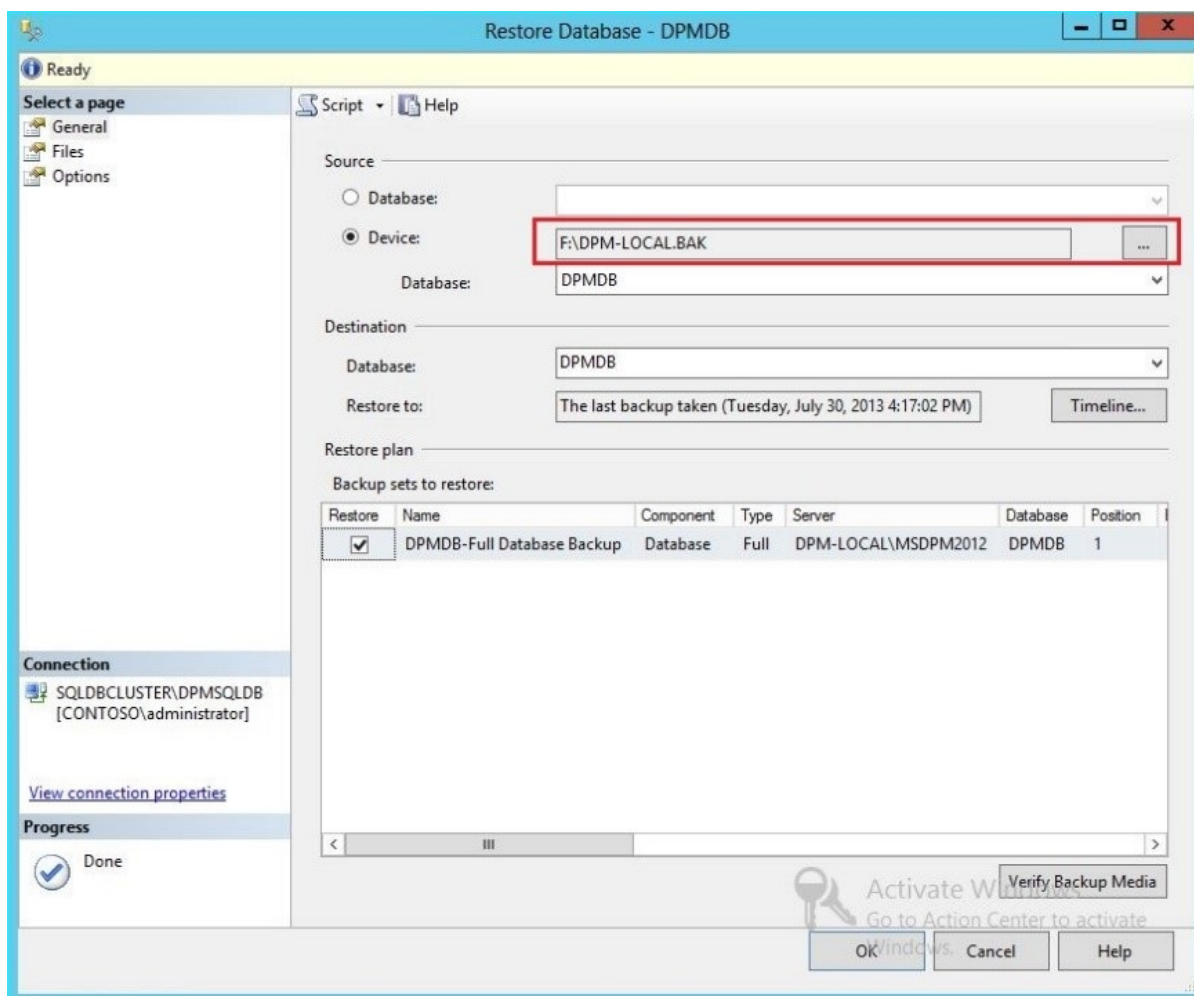
3. Dodaj miejsce docelowe kopii zapasowej i nazwę pliku, a następnie wybierz pozycję **OK**, aby rozpocząć tworzenie kopii zapasowej.



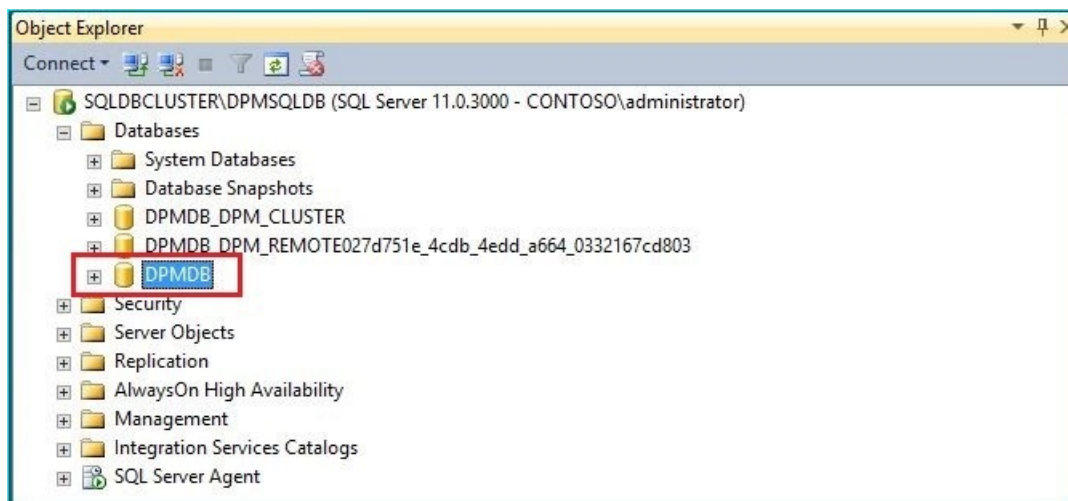
4. Po wykonaniu kopii zapasowej skopiuj plik wyjściowy do zdalnego programu SQL Server. Jeśli jest to klaster programu SQL, skopiuj go do aktywnego węzła hostującego wystąpienie programu SQL, którego chcesz użyć podczas uaktualniania programu DPM. Zanim będzie można wykonać przywracanie, należy skopiować kopię zapasową na udostępniony dysk klastra.
5. Na maszynie zdalnego programu SQL Server uruchom program **Microsoft SQL Management Studio** i połącz się z wystąpieniem programu SQL, którego chcesz użyć podczas uaktualniania programu DPM. Jeśli jest to klaster programu SQL, należy to zrobić w aktywnym węźle, do którego skopiowano plik kopii zapasowej. Plik kopii zapasowej teraz powinien znajdować się na udostępnionym dysku klastra.
6. Kliknij prawym przyciskiem myszy ikonę Bazy danych, a następnie wybierz polecenie **Przywróć bazę danych...**. Spowoduje to uruchomienie kreatora przywracania.



7. Wybierz pozycję **Urządzenie** w obszarze **Źródło**, a następnie znajdź plik kopii zapasowej bazy danych, który został skopiowany w poprzednim kroku, i wybierz go. Zweryfikuj opcje i lokalizację przywracania, a następnie wybierz pozycję **OK**, aby rozpocząć przywracanie. Rozwiąż wszelkie problemy zgłoszone podczas przywracania, aby zakończyć je pomyślnie.



8. Po zakończeniu przywracania przywrócona baza danych będzie widoczna w obszarze **Bazy danych** pod oryginalną nazwą. Ta baza danych zostanie użyta podczas uaktualniania. Możesz zakończyć program **Microsoft SQL Management Studio** i uruchomić proces uaktualniania na oryginalnym serwerze programu DPM.



9. Jeśli nowy program SQL Server jest zdalny, zainstaluj narzędzia zarządzania programem SQL na serwerze programu DPM. Wersja narzędzi zarządzania programem SQL musi pasować do wersji programu SQL Server hostującego bazę danych DPMDB.

Uruchomienie uaktualnienia w celu zmigrowania bazy danych DPMDB do innego programu SQL Server

NOTE

Jeśli wystąpienie programu SQL jest współużytkowane, uruchom instalację lub uaktualnienia programu DPM sekwencyjnie. Instalowanie równoległe może spowodować wystąpienie błędów.

1. Po zakończeniu kroków przygotowania przed migracją uruchom proces instalacji programu DPM 2016. Instalator programu DPM wyświetla informacje o bieżącym wystąpieniu programu SQL Server. W tym miejscu możesz wybrać inne wystąpienie programu SQL Server lub przejść na klastrowe wystąpienie programu SQL używane podczas migracji.

Data Protection Manager Setup

Prerequisites Check

Please wait while the wizard checks for required hardware and software.

Installation Stages

- Welcome
- Prerequisites check
- Product registration
- Installation settings
- Microsoft Update Opt-In
- Customer feedback option
- Installation

DPM requires a database. You can use a local or remote instance of SQL Server that already exists.

☒ Use stand-alone SQL Server.
SQL Server is not clustered.

☐ Use clustered SQL Server
SQL Server is clustered

Instance of SQL Server
(Example: SQLSERV or SQLSERV\MYSQLINSTANCE):

User Name: Password:

Domain:

Select the appropriate option and click on the button to perform the prerequisite check and install the missing Windows components.

< Back Next > Cancel Help

2. Zmień ustawienia programu SQL, aby użyć wystąpienia programu SQL Server, do którego przywrócono bazę danych DPM. Jeśli jest to klaster programu SQL, musisz także określić osobne wystąpienie programu SQL Server używane na potrzeby raportowania programu SQL. Przyjęto, że wszystkie reguły zapory oraz program SQLPrep zostały już uruchomione. Musisz podać poprawne poświadczenia, a następnie kliknąć przycisk **Sprawdź i instaluj**.

Data Protection Manager Setup

Prerequisites Check

Please wait while the wizard checks for required hardware and software.

Installation Stages

- Welcome
- Prerequisites check
- Product registration
- Installation settings
- Microsoft Update Opt-In
- Customer feedback option
- Installation

DPM requires a database. You can use a local or remote instance of SQL Server that already exists.

☐ Use stand-alone SQL Server.
SQL Server is not clustered.

☒ Use clustered SQL Server
SQL Server is clustered

Instance of SQL Server
(Example: SQLSERV or SQLSERV\MYSQLINSTANCE):

User Name: Password:

Domain:

Instance of SQL Server Reporting Service
(Example: SQLSERV or SQLSERV\MYREPORTINGINSTANCE):

User Name: Password:

Domain:

Select the appropriate option and click on the button to perform the prerequisite check and install the missing Windows components.

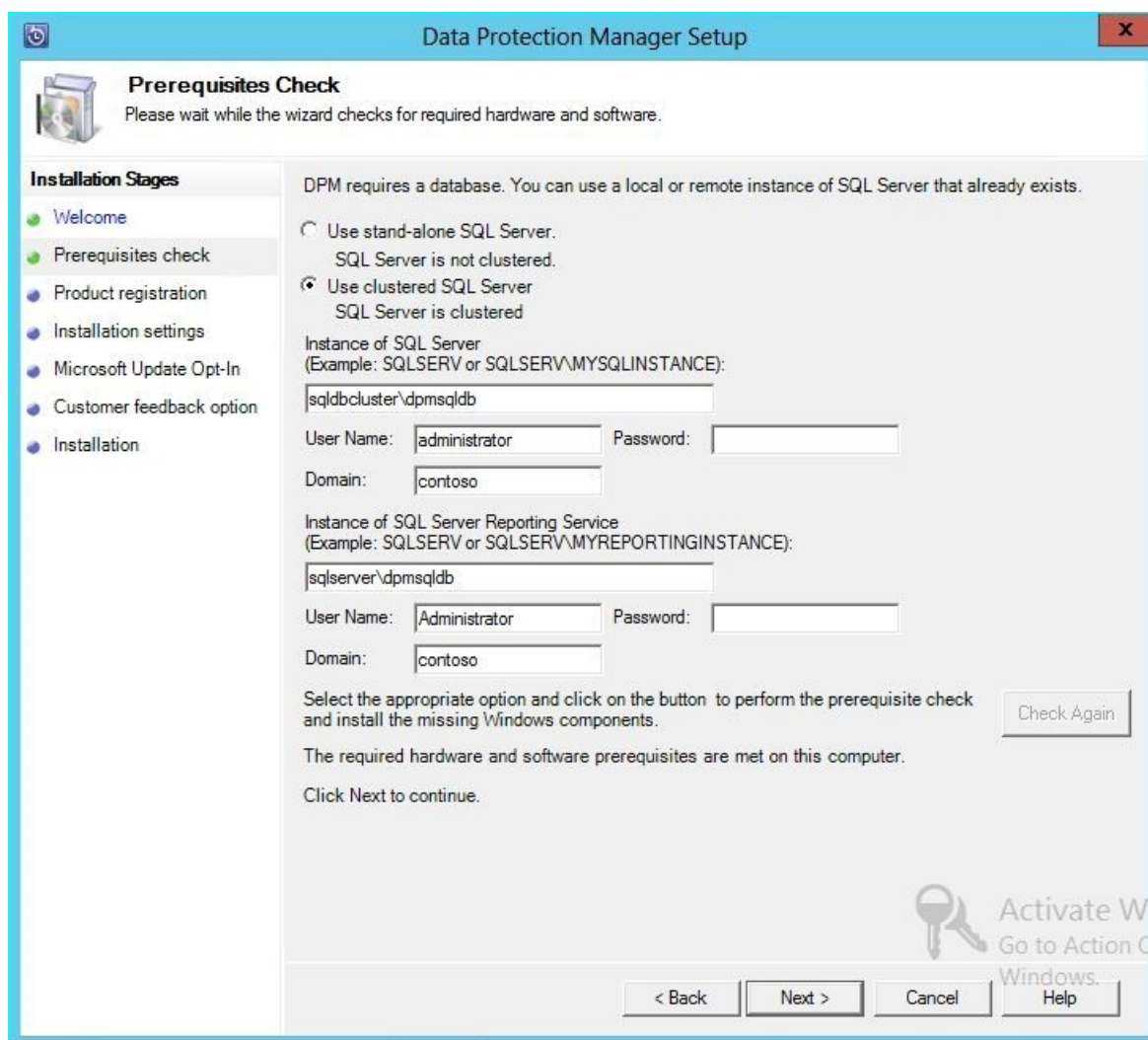
Check and Install

Details

 Setup will use the current user's credentials for this SQL instance.

< Back Next > Cancel Help

3. Sprawdzanie wymagań wstępnych powinno zakończyć się pomyślnie. Naciśnij pozycję DALEJ, aby kontynuować uaktualnianie.



4. Kontynuuj pracę kreatora.
5. Po zakończeniu instalacji odpowiadająca baza danych w ramach określonego wystąpienia będzie miała teraz nazwę DPMPB_DPMNazwaSerwera. Ponieważ może być ona współużytkowana z innymi serwerami programu DPM, konwencja nazewnictwa dla bazy danych DPM będzie teraz następująca:
DPM2016\$DPMDB_DPMNazwaSerwera

Dodawanie miejsca do magazynowania dla funkcji Modern Backup Storage

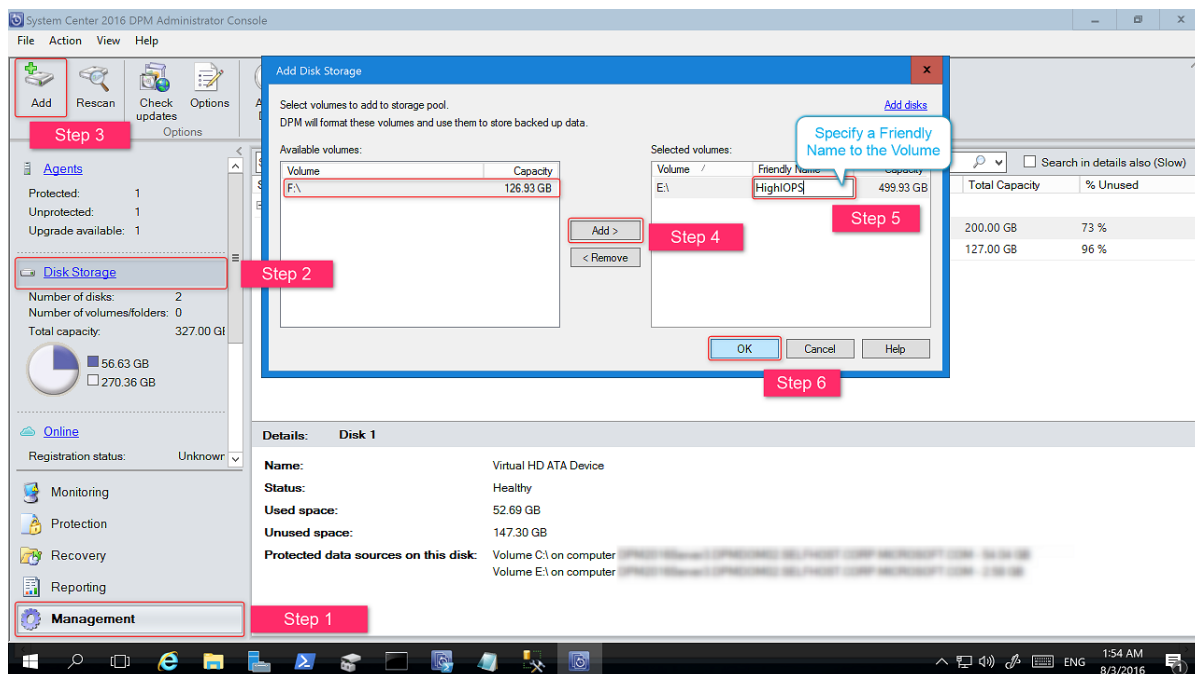
Aby wydajnie przechowywać kopie zapasowe, program DPM 2016 używa woluminów. Można także kontynuować przechowywanie kopii zapasowych na dyskach, jak w programie DPM 2012 R2.

Dodawanie woluminów i dysków

Jeśli uruchamiasz program DPM 2016 w systemie Windows Server, możesz przechowywać dane kopii zapasowych na woluminach. Woluminy pozwalają zaoszczędzić miejsce do magazynowania i zapewniają szybsze tworzenie kopii zapasowych. Możesz nadać woluminowi przyjazną nazwę i możesz zmienić jego nazwę. Podaj przyjazną nazwę podczas dodawania woluminu lub później, klikając kolumnę **Przyjazna nazwa** wybranego woluminu. Za pomocą programu PowerShell także można dodawać i zmieniać przyjazne nazwy dla woluminów.

Aby dodać wolumin w konsoli administratora:

1. W konsoli administratora programu DPM wybierz funkcję **Zarządzanie**, a następnie wybierz pozycję **Magazyn dyskowy > Dodaj**.
2. W oknie dialogowym **dodawanie Disk Storage** wybierz dostępny wolumin > kliknij przycisk **Dodaj** > Wpisz przyjazną nazwę woluminu > kliknij przycisk **OK**.



Jeśli chcesz dodać dysk, musi on należeć do grupy ochrony ze starszą wersją magazynu. Te dyski mogą być używane tylko dla tych grup ochrony. Jeśli serwer programu DPM nie ma źródła ze starszą ochroną, dysk nie będzie widoczny. Aby uzyskać więcej informacji na temat dodawania dysków, zobacz [Dodawanie dysków w celu zwiększenia miejsca w starszej wersji magazynu](#). Dyskowi nie można nadać przyjaznej nazwy.

Przypisywanie obciążeń do woluminów

Program DPM 2016 umożliwia użytkownikowi określenie, jakie rodzaje obciążeń powinny być przypisane do poszczególnych woluminów. Na przykład kosztowne woluminy, które obsługują bardzo duże liczby operacji we/wy na sekundę, można skonfigurować tak, aby przechowywały tylko obciążenia wymagające częstego tworzenia dużych kopii zapasowych, jak w przypadku programu SQL z dziennikami transakcji. Aby zaktualizować właściwości woluminu w puli magazynów na serwerze programu DPM, użyj polecenia cmdlet programu PowerShell: Update-DPMDiskStorage.

Update-DPMDiskStorage

Składnia

Parameter Set: Volume

```
Update-DPMDiskStorage [-Volume] <Volume> [[-FriendlyName] <String> ] [[-DatasourceType] <VolumeTag[]> ] [-Confirm] [-WhatIf] [ <CommonParameters>]
```

Zmiany wprowadzone za pomocą programu PowerShell są odzwierciedlane w interfejsie użytkownika.

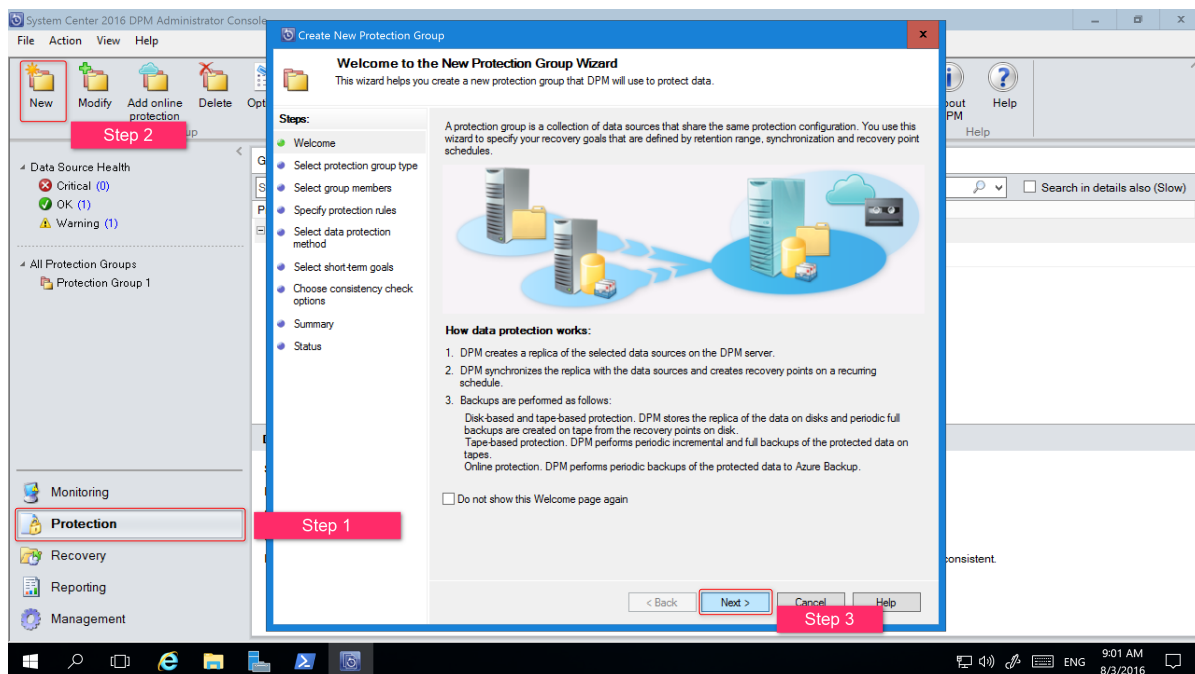
Ochrona źródeł danych

Aby rozpocząć ochronę źródeł danych, utwórz grupę ochrony. Poniższa procedura podkreśla zmiany i dodatki w kreatorze **Nowa grupa ochrony**.

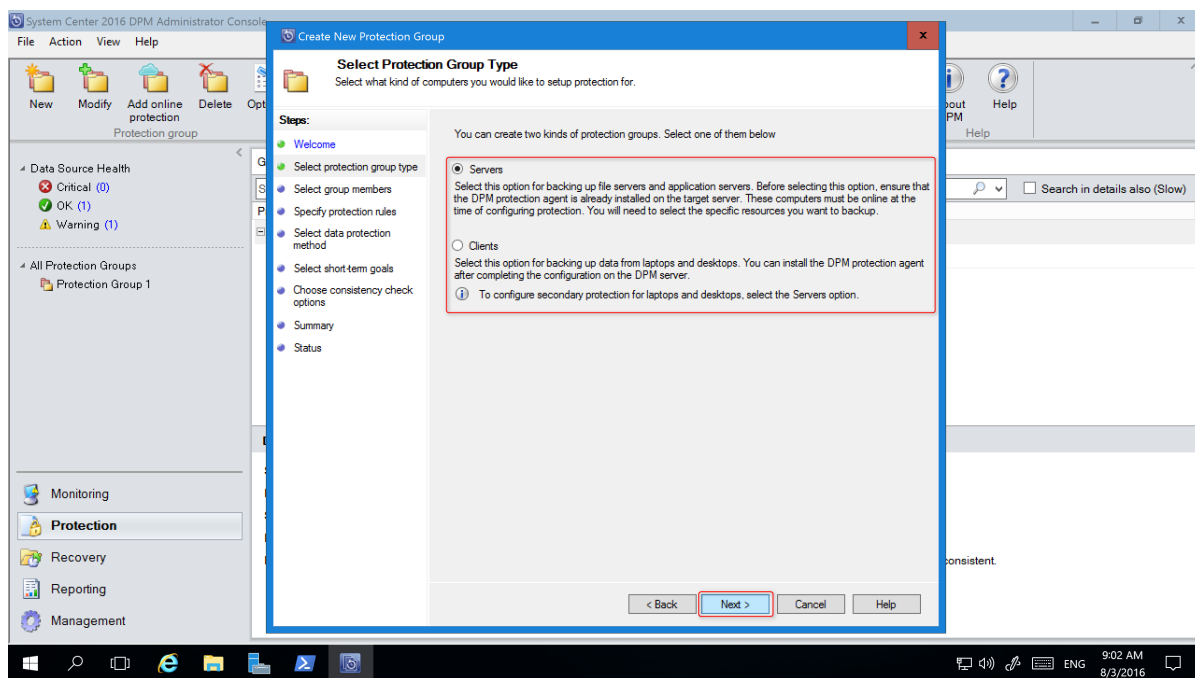
Aby utworzyć grupę ochrony:

1. W konsoli administratora programu DPM wybierz funkcję **Ochrona**.
2. Na wstążce narzędzi kliknij pozycję **Nowy**.

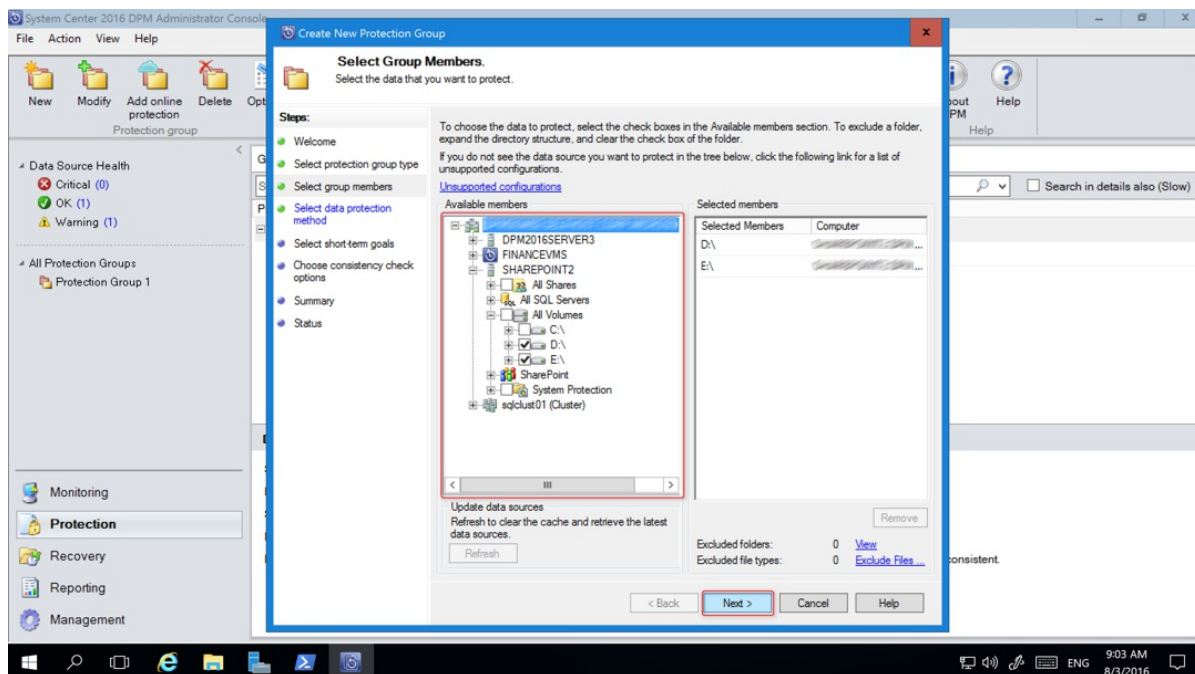
Zostanie otwarty kreator **Utwórz nową grupę ochrony**.



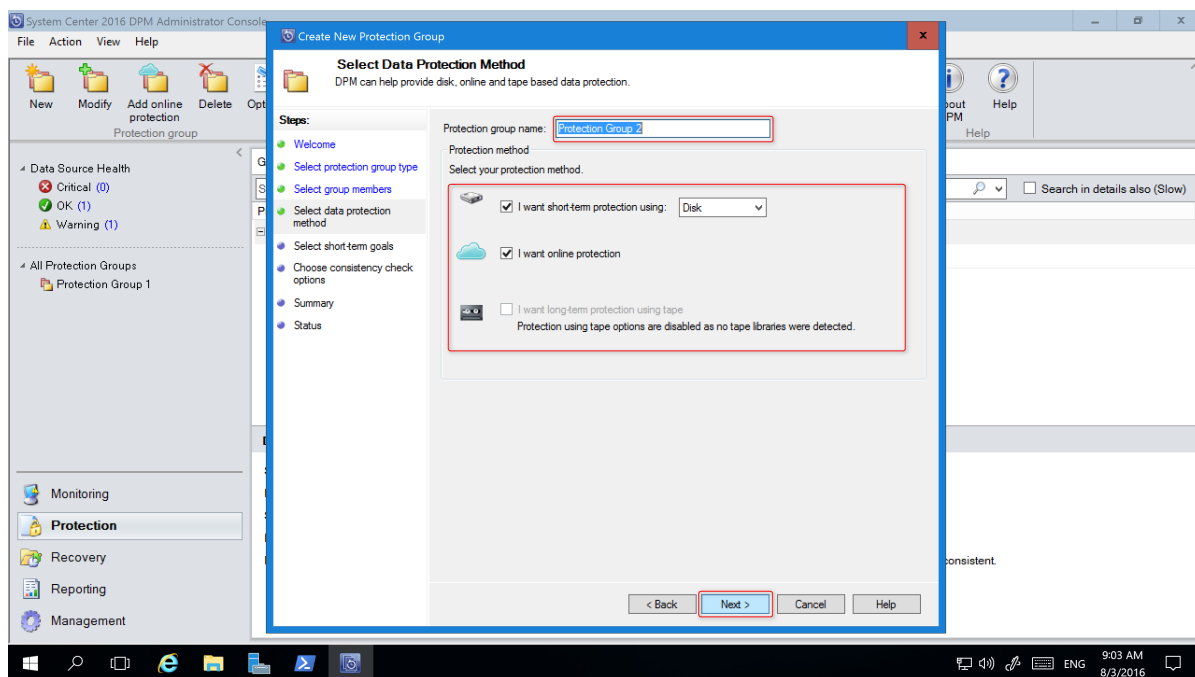
3. Kliknij przycisk **Dalej**, aby przejść w kreatorze do ekranu **Wybierz typ grupy ochrony**.
4. Na ekranie **Wybierz typ grupy ochrony** wybierz typ grupy ochrony, który ma zostać utworzony, a następnie kliknij przycisk **Dalej**.



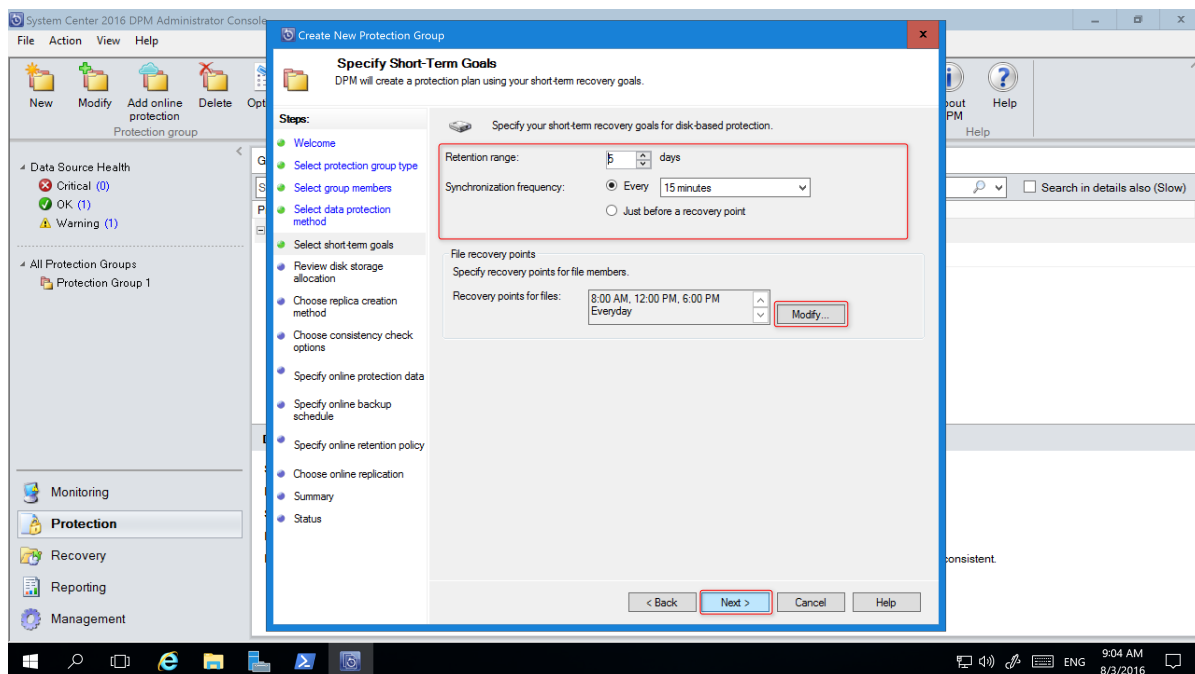
5. Na ekranie **Wybierz elementy członkowskie grupy** w okienku **Dostępne elementy członkowskie** program DPM wyświetla listę elementów członkowskich z agentami ochrony. Na potrzeby tego przykładu wybierz woluminy D:\ i E:, aby dodać je do okienka **Wybrane elementy członkowskie**. Po wybraniu elementów członkowskich do grupy ochrony kliknij przycisk **Dalej**.



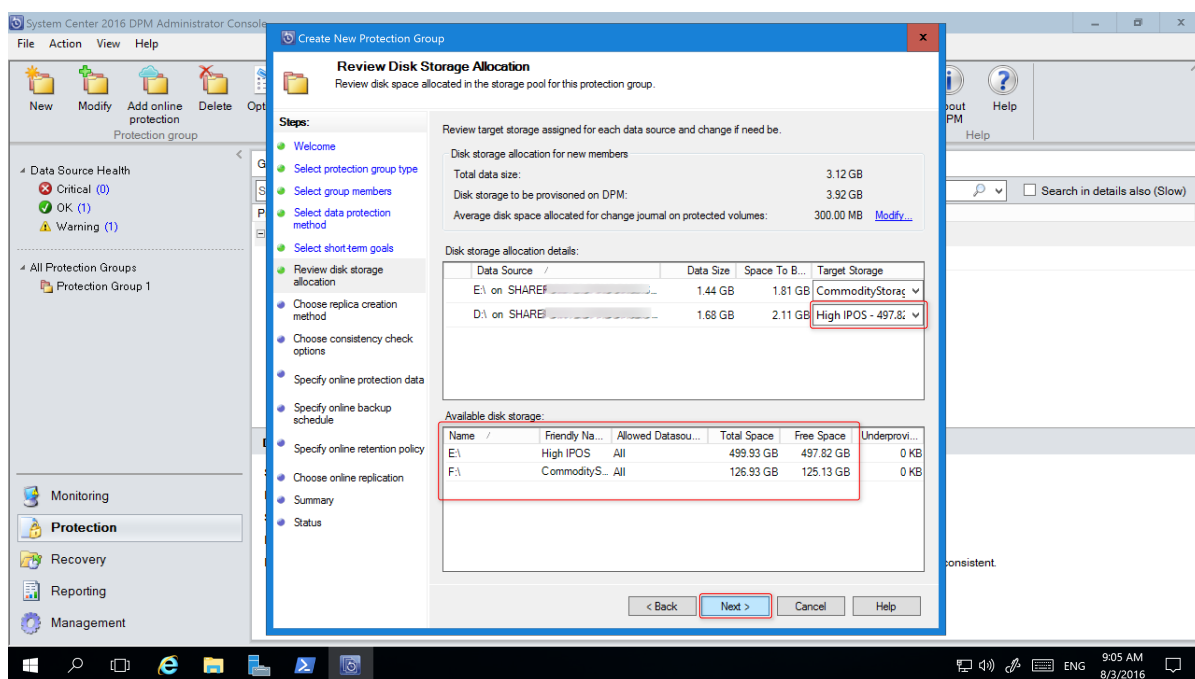
6. Na ekranie **Wybierz metodę ochrony danych** w polu **Grupa ochrony** wpisz nazwę grupy ochrony, wybierz metody ochrony i kliknij przycisk **Dalej**. Jeśli chcesz ochrony krótkoterminowej, musisz użyć kopii zapasowej dysku.



7. Na ekranie **Określ cele krótkoterminowe** określ szczegóły w polach **Zakres przechowywania** i **Częstotliwość synchronizacji**, a następnie kliknij przycisk **Dalej**. Jeśli chcesz, kliknij przycisk **Modyfikuj**, aby zmienić harmonogram wykonywania punktów odzyskiwania.

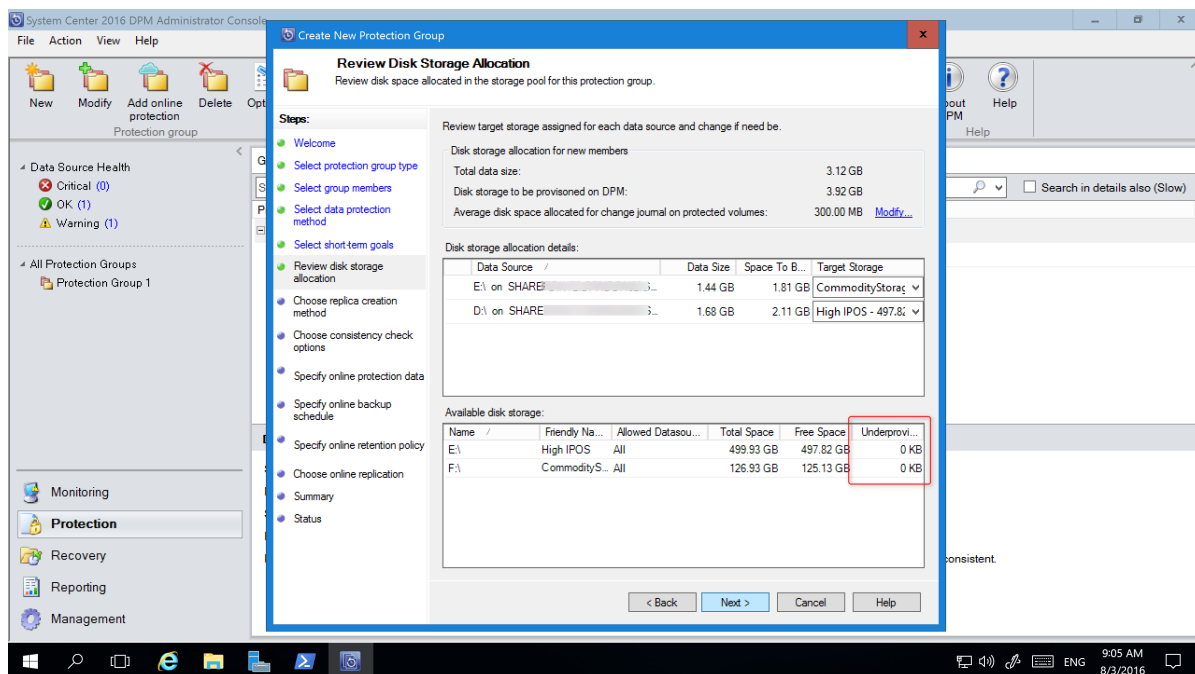


8. Ekran **Przejrzyj przydział magazynu dyskowego** zawiera szczegółowe informacje dotyczące wybranych źródeł danych i ich wielkości oraz dane w obszarach **Miejsce na potrzeby aprowizacji** i **Docelowy wolumin magazynu**.



Woluminy magazynu są określane na podstawie alokacji woluminu obciążenia (ustawianego przy użyciu programu PowerShell) i dostępnego miejsca do magazynowania. Woluminy magazynu można zmienić, wybierając inne woluminy z menu rozwijanego. Jeśli zmienisz wartość w polu **Magazyn docelowy**, dane w polu **Dostępny magazyn dyskowy** zmieniają się dynamicznie, aby odzwierciedlić wartości w polach **Wolne miejsce** i **Miejsce poniżej aprowizacji**.

Kolumna **Miejsce poniżej aprowizacji** w obszarze **Dostępny magazyn dyskowy** odzwierciedla ilość dodatkowego miejsca, które będzie potrzebne, jeśli źródła danych zwiększą się zgodnie z planem. Użyj tej wartości, aby pomóc w zaplanowaniu potrzeb magazynowych w celu umożliwienia bezproblemowego tworzenia kopii zapasowych. Jeśli ta wartość wynosi zero, oznacza to, że w najbliższej przyszłości nie ma potencjalnych problemów z magazynem. Jeśli wartość jest różna od zera, oznacza to, że przydzielone miejsce w magazynie nie jest wystarczające — na podstawie zasad ochrony i rozmiaru danych chronionych elementów członkowskich.

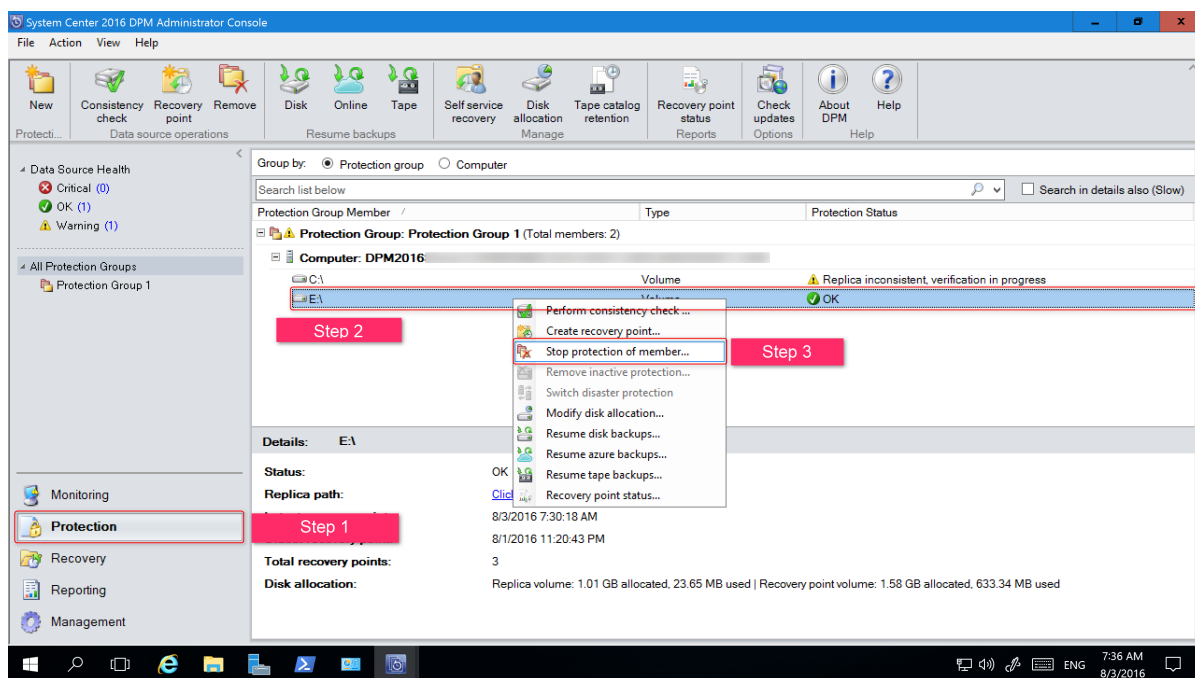


Pozostała część Kreatora nowej grupy ochrony jest taka sama, jak w programie DPM 2012 R2. Kontynuuj wykonywanie kroków kreatora, aby ukończyć tworzenie nowej grupy ochrony.

Migrowanie starszej wersji magazynu do funkcji Modern Backup Storage

Po uaktualnieniu programu DPM 2012 R2 do programu DPM 2016 i systemu operacyjnego do wersji Windows Server 2016 można zaktualizować istniejące grupy ochrony do nowych funkcji programu DPM 2016. Domyślnie grupy ochrony nie są zmieniane i nadal funkcjonują tak, jak zostały skonfigurowane w programie DPM 2012 R2. Aktualizowanie grup ochrony w celu korzystania z funkcji Modern Backup Storage jest opcjonalne. Aby zaktualizować grupę ochrony, zatrzymaj ochronę wszystkich źródeł danych z opcją zachowania danych, a następnie dodaj źródła danych do nowej grupy ochrony. Program DPM zacznie chronić te źródła danych w nowy sposób.

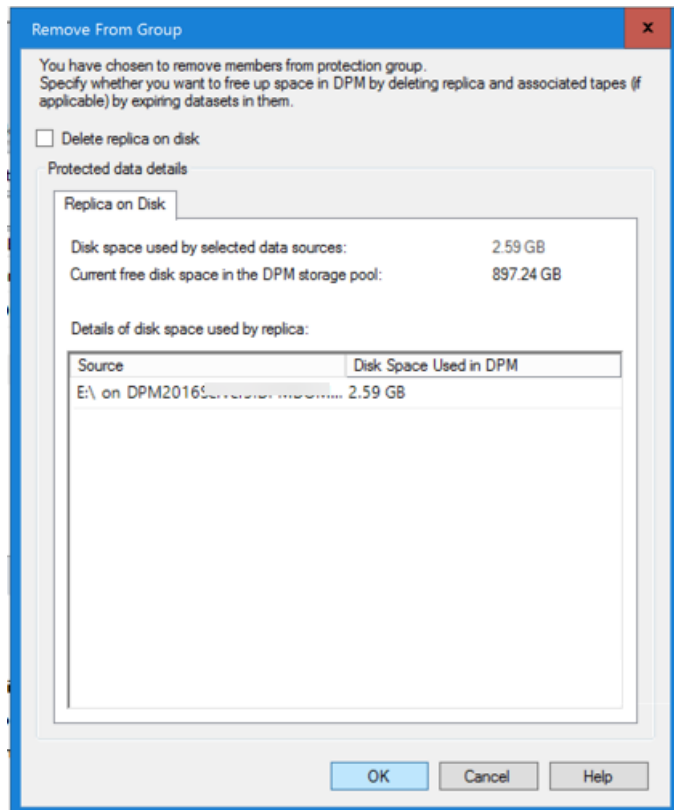
1. W konsoli administratora wybierz funkcję **Ochrona** i na liście **Element członkowski grupy ochrony** kliknij prawym przyciskiem myszy wybrany element członkowski, a następnie wybierz polecenie **Zatrzymaj ochronę elementu członkowskiego**.



Zostanie otwarte okno dialogowe **Usuń z grupy**.

2. W oknie dialogowym **Usuń z grupy** przejrzyj używane miejsce na dysku i dostępne wolne miejsce w puli magazynów. Domyślnie punkty odzyskiwania pozostają na dysku i wygasają zgodnie ze skojarzonymi z nimi zasadami przechowywania. Kliknij przycisk **OK**.

Aby natychmiast przywrócić zajęte miejsce na dysku do wolnej puli magazynów, zaznacz opcję **Usuń replikę z dysku**. Spowoduje to usunięcie danych kopii zapasowej (i punktów odzyskiwania) skojarzonych z tym elementem członkowskim.



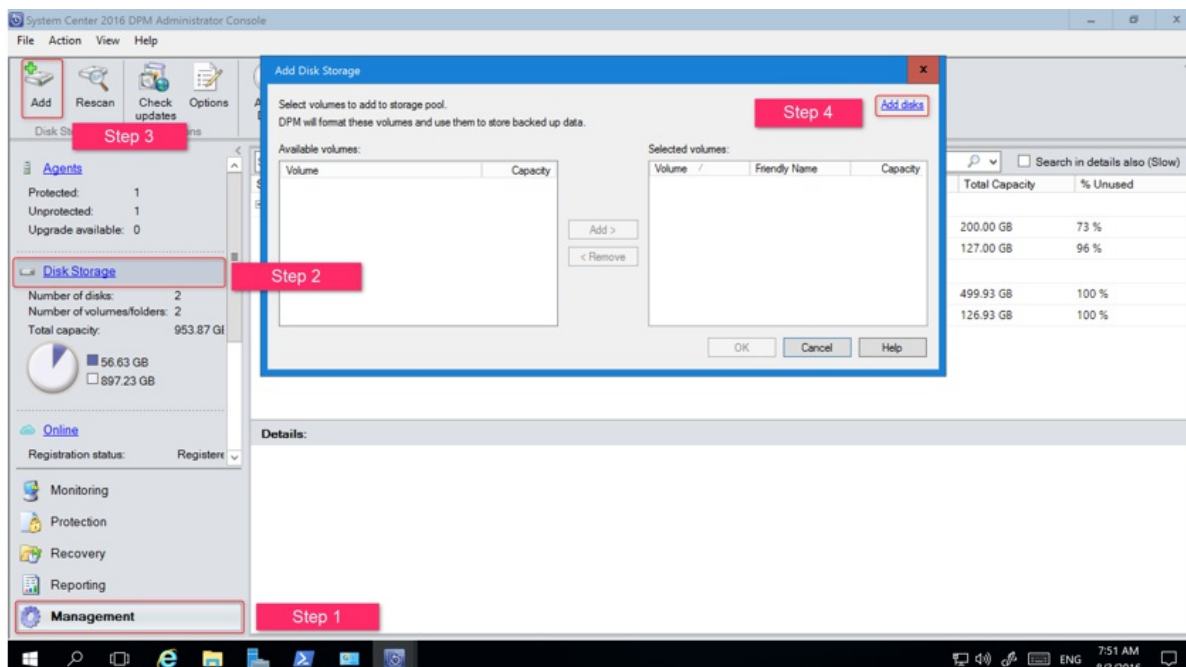
3. Utwórz nową grupę ochrony, która używa Nowoczesny magazyn kopii zapasowych i Uwzględnij niechronione źródła danych.

Dodawanie dysków w celu zwiększenia magazynu w starszej wersji

Jeśli chcesz używać starszej wersji magazynu z programem DPM 2016, może być konieczne dodanie dysków w celu zwiększenia magazynu w starszej wersji. Aby dodać magazyn dyskowy:

1. W konsoli administratora kliknij pozycję **Zarządzanie**.
2. Wybierz pozycję **Magazyn dyskowy**.
3. Na wstążce narzędzi kliknij pozycję **Nowy**.

Zostanie otwarte okno dialogowe **Dodawanie magazynu dyskowego**.



4. W oknie dialogowym **Dodawanie magazynu dyskowego** kliknij pozycję **Dodaj dyski**.

Program DPM wyświetli listę dostępnych dysków.

5. Wybierz dyski, kliknij przycisk **Dodaj**, aby dodać te dyski, a następnie kliknij przycisk **OK**.

Nowe polecenia cmdlet programu PowerShell

W programie DPM 2016 dostępne są dwa nowe polecenia cmdlet: [Mount-DPMRecoveryPoint](#) i [Dismount-DPMRecoveryPoint](#). Kliknij nazwę polecenia cmdlet, aby wyświetlić dotyczącą go dokumentację.

Włączanie ochrony w chmurze

Kopię zapasową serwera programu DPM można utworzyć na platformie Azure. Ogólna procedura jest następująca:

- Utwórz subskrypcję platformy Azure.
- Zarejestruj serwer w usłudze Kopia zapasowa Azure.
- Pobierz poświadczenia magazynu i agenta kopii zapasowej Azure.
- Skonfiguruj poświadczenia magazynu i zasady tworzenia kopii zapasowej serwera.

Aby uzyskać więcej informacji na temat tworzenia kopii zapasowych programu DPM w chmurze, zapoznaj się z artykułem [przygotowanie do tworzenia kopii zapasowych obciążeń na platformie Azure przy użyciu programu DPM](#).

Następne kroki

Dowiedz się, jak [dodać magazyn](#).

Dodawanie Nowoczesny magazyn kopii zapasowych do programu DPM

06.03.2020 • 27 minutes to read

Nowoczesny magazyn kopii zapasowych (MB) została wprowadzona w programie System Center Data Protection Manager (DPM) 2016, aby dostarczyć 50% oszczędności za magazyn, 3. szybsze kopie zapasowe i wydajny magazyn z obsługą obciążeń.

- MB jest włączana automatycznie w przypadku uruchomienia co najmniej programu DPM 2016 w systemie Windows Server 2016. Jeśli program DPM jest uruchomiony w wersji systemu Windows Server starszej niż Windows Server 2016, nie używa MB.
- MB zapewnia inteligentny magazyn do krótkoterminowej kopii zapasowej na dysku. MB zapewnia szybszą kopię zapasową dysku, zużywając mniej miejsca na dysku. Bez MB każdego źródła danych wymagane są dwa woluminy, jeden dla początkowej kopii zapasowej, a drugi dla zmian różnicowych.
- Kopie zapasowe MB są przechowywane na dysku systemu plików ReFS. Używa ona klonowania bloków systemu plików ReFS i technologii VHDX, [Dowiedz się więcej](#).

NOTE

Program DPM nie obsługuje deduplikacji na dysku ReFS używanym do tworzenia kopii zapasowych MB.

Program DPM 2016 akceptuje woluminy na potrzeby magazynu. Po dodaniu woluminu program DPM sformatuje wolumin do systemu plików ReFS, aby korzystać z nowych funkcji Nowoczesny magazyn kopii zapasowych. Woluminy nie mogą znajdować się na dysku dynamicznym. Używaj tylko dysku podstawowego.

Mimo że możesz bezpośrednio przekazać wolumin do programu DPM, możesz obsługiwać problemy z rozszerzaniem woluminu, jeśli będzie to konieczne w przyszłości. Aby przygotować program DPM do późniejszego rozbudowy, użyj dostępnych dysków, aby utworzyć pulę magazynu, a następnie utwórz woluminy w puli magazynów i uwidocznić woluminy w programie DPM. Te woluminy wirtualne można następnie rozszerzać w razie konieczności.

Pozostała część tego artykułu zawiera szczegółowe informacje dotyczące sposobu dodawania woluminu i rozszerzania go później.

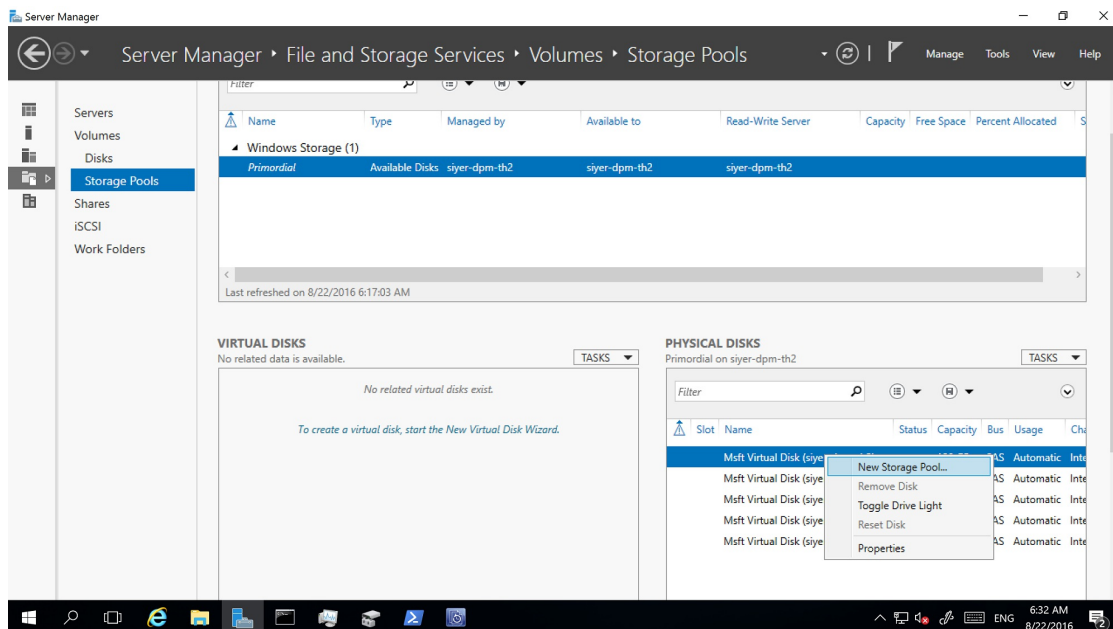
Konfigurowanie MB

Konfigurowanie MB składa się z następujących procedur. Należy pamiętać, że nie można dołączyć lokalnie utworzonych plików VHD (VHDX) i używać ich jako magazynu na fizycznym serwerze programu DPM.

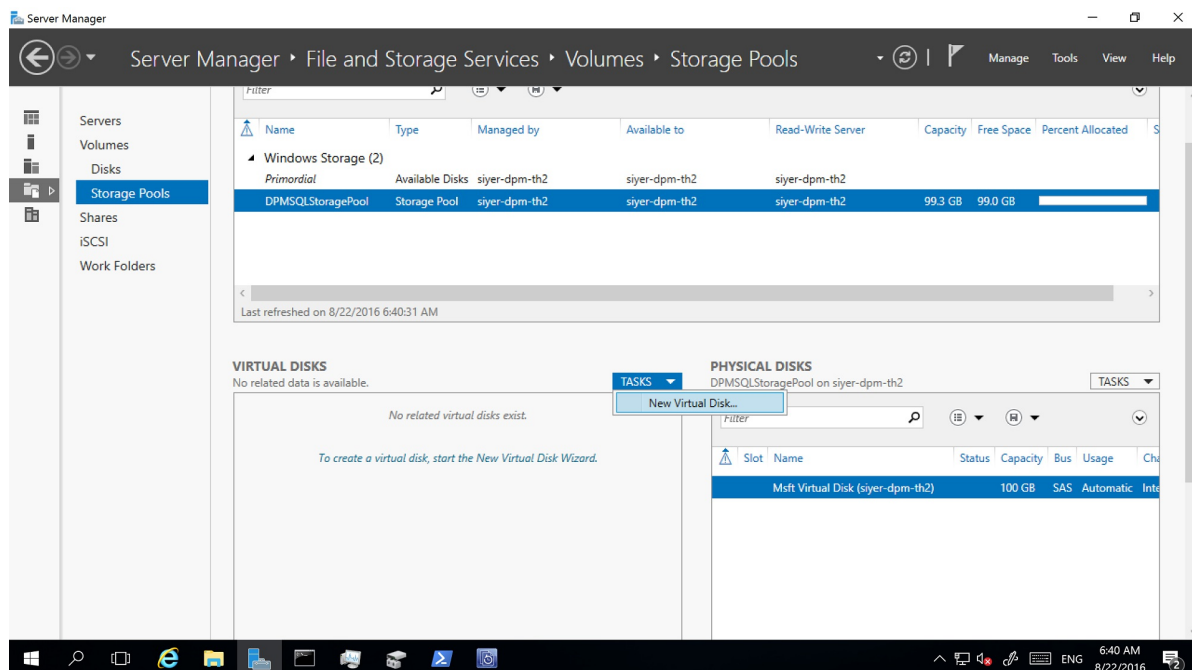
1. Upewnij się, że korzystasz z programu DPM 2016 lub nowszego na maszynie wirtualnej z systemem Windows Server 2016 lub nowszym.
2. Utwórz wolumin. Aby utworzyć wolumin na dysku wirtualnym w puli magazynu:
 - Dodawanie dysku do puli magazynów
 - Utwórz dysk wirtualny z puli magazynów z ustawionym układem na prosty. Następnie można dodać dodatkowe dyski lub zwiększyć dysk wirtualny.
 - Utwórz woluminy na dysku wirtualnym.
3. Dodaj woluminy do programu DPM.
4. Skonfiguruj magazyn obsługujący obciążenie.

Tworzenie woluminu

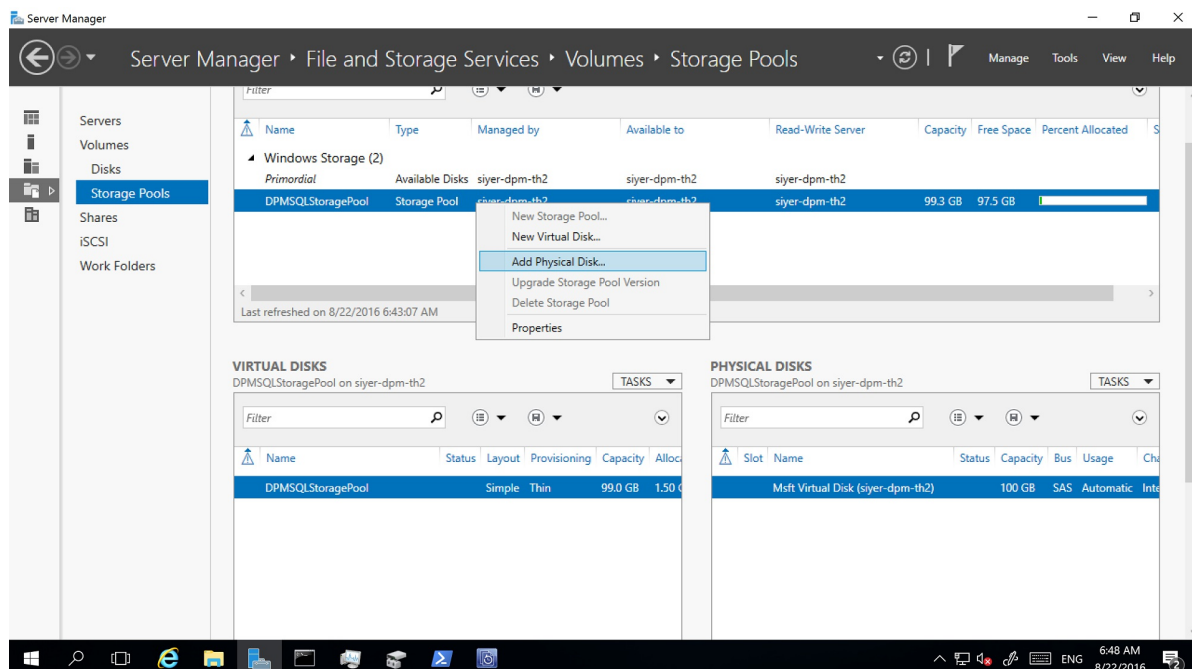
1. Utwórz pulę magazynów w usłudze plików i magazynowania Menedżer serwera.
2. Dodaj dostępne dyski fizyczne do puli magazynów.
 - Dodanie tylko jednego dysku do puli zachowuje liczbę kolumn na 1. Następnie można dodać dyski odpowiednio do wymagań.
 - Jeśli do puli magazynów dodano wiele dysków, liczba dysków jest przechowywana jako liczba kolumn. Po dodaniu większej liczby dysków może to być tylko wielokrotność liczby kolumn.



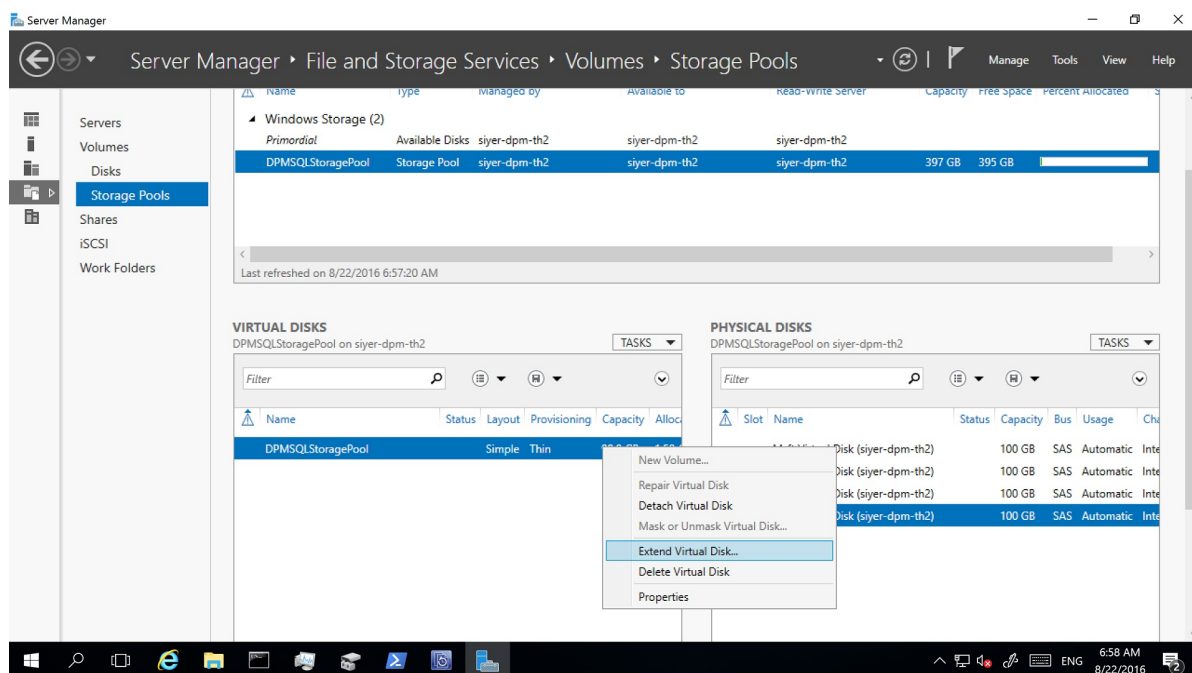
3. Utwórz dysk wirtualny z puli magazynów, z układem ustawionym na prosty.



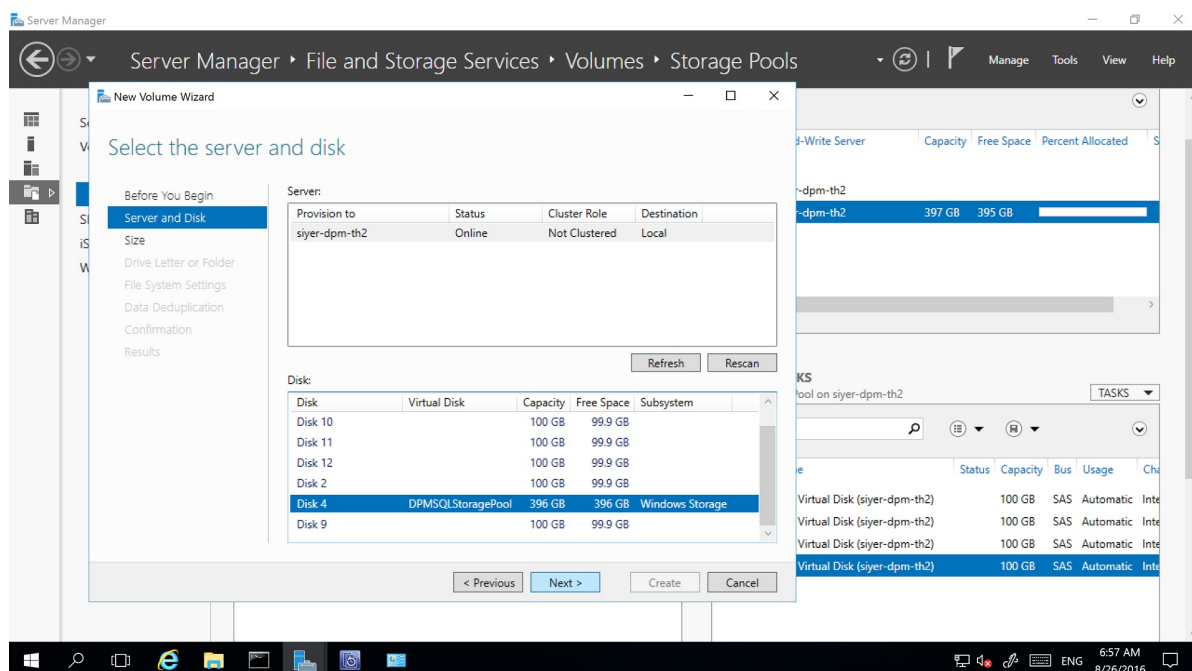
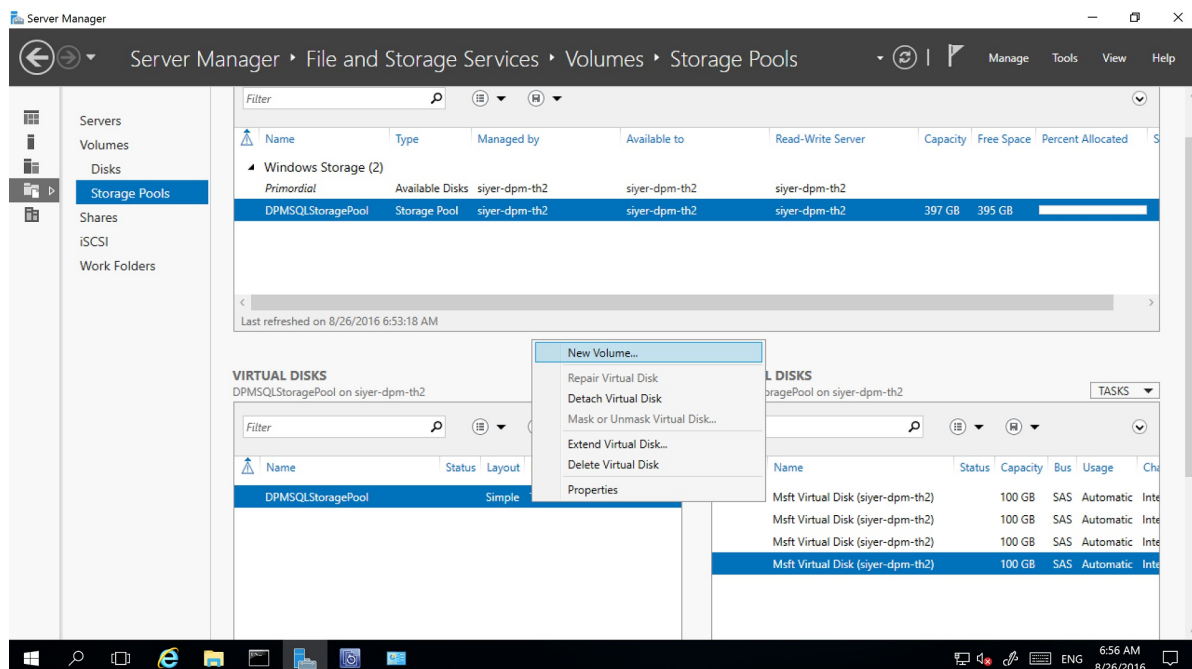
4. Teraz Dodaj dowolną liczbę dysków fizycznych.



5. Zwiększ dysk wirtualny przy użyciu układu prostego, aby odzwierciedlić wszystkie dodane dyski fizyczne.

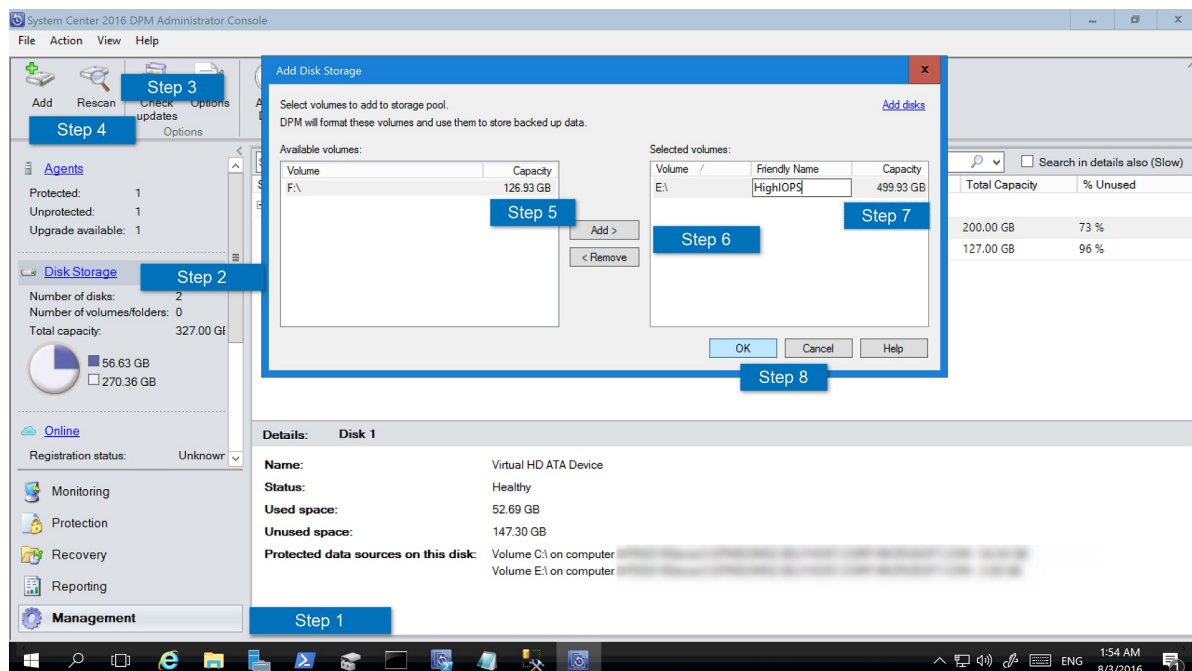


6. Teraz Utwórz woluminy na dysku wirtualnym.



Dodawanie woluminów do magazynu programu DPM

1. W konsoli zarządzania programu DPM > **Disk Storage** kliknij pozycję **Skanuj** ponownie.
2. W obszarze **dodaj Disk Storage** kliknij pozycję **Dodaj**.
3. Po dodaniu woluminów można nadać im przyjazną nazwę.
4. Kliknij przycisk **OK**, aby sformatować woluminy do systemu plików ReFS, aby program DPM mógł ich używać jako MB.



Konfigurowanie magazynu obsługującego obciążenie

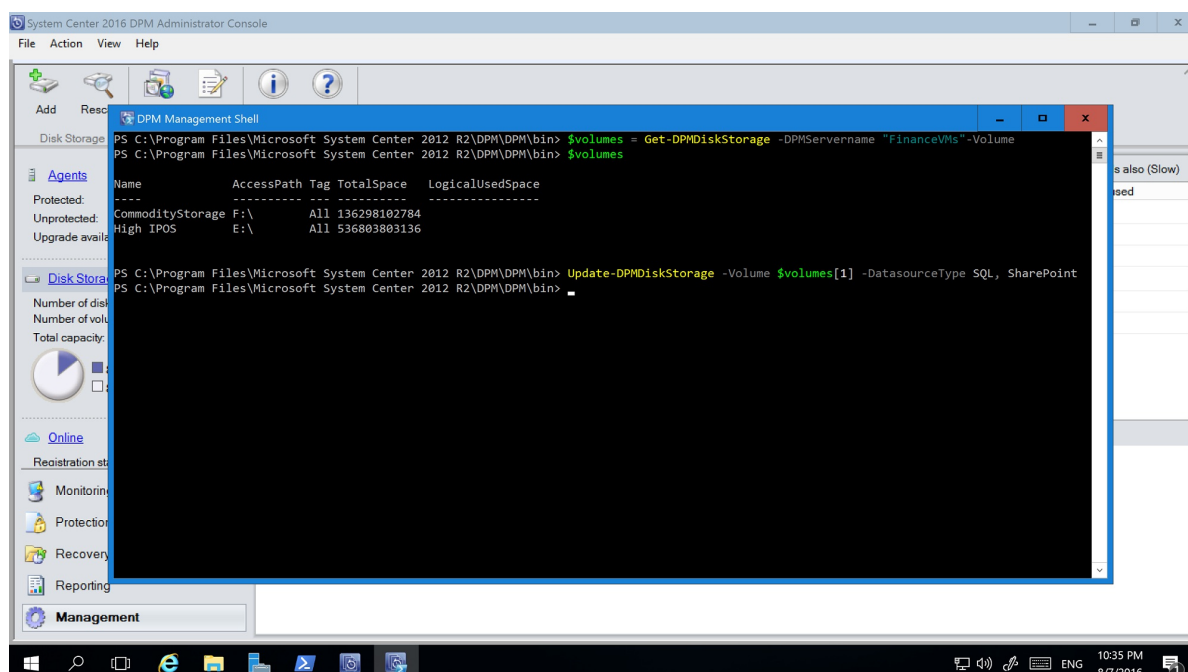
Korzystając z magazynu obsługującego obciążenie, można wybierać woluminy w celu preferencyjnego przechowywania określonych obciążeń. Na przykład drogie woluminy obsługujące dużą liczbę IOPS można skonfigurować do przechowywania obciążeń wymagających częstych kopii zapasowych, takich jak SQL Server z dziennikami transakcji. W przypadku obciążeń, dla których kopie zapasowe są tworzone rzadziej, takich jak maszyny wirtualne, można utworzyć kopię zapasową na woluminach o niskim koszcie.

Magazyn z obsługą obciążeń można skonfigurować przy użyciu poleceń cmdlet programu Windows PowerShell.

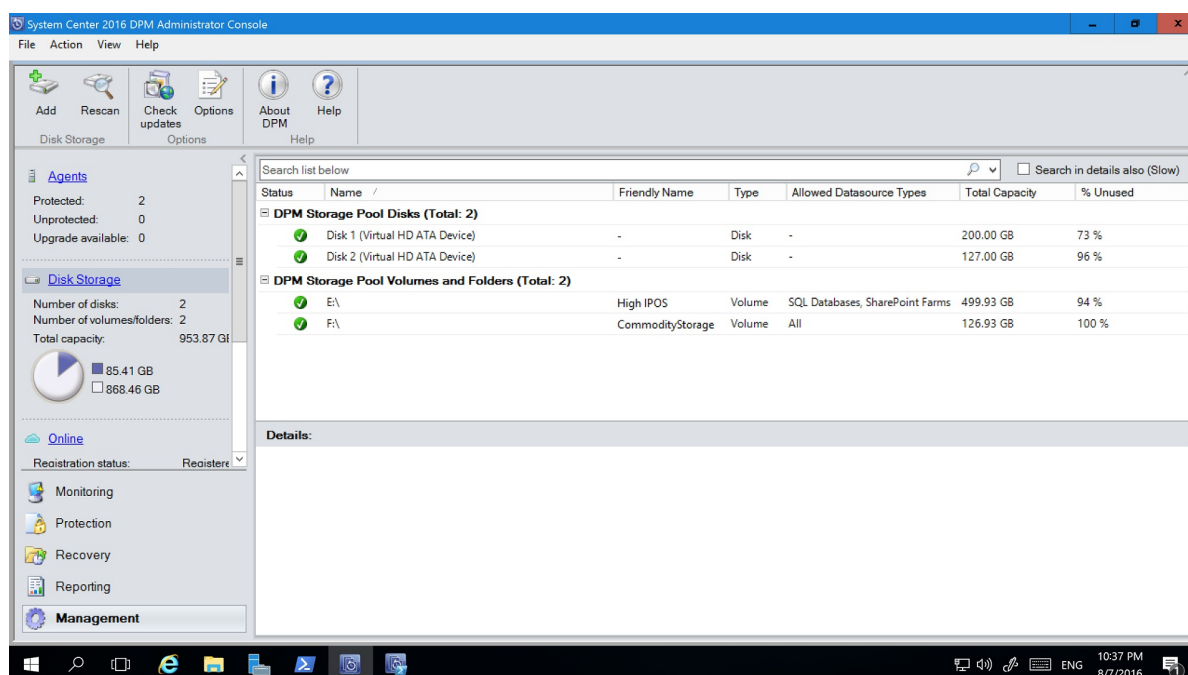
Aktualizowanie właściwości woluminu

1. Uruchom **aktualizację Update-DPMDiskStorage**, aby zaktualizować właściwości woluminu w puli magazynów na serwerze programu DPM. Składnia to **zestaw parametrów: wolumin**.
2. Uruchom polecenie cmdlet z tymi parametrami.

```
Update-DPMDiskStorage [-Volume] <Volume> [[-FriendlyName] <String> ] [[-DatasourceType] <VolumeTag[]> ]
[-Confirm] [-WhatIf] [ <CommonParameters>]
```

3. Zmiany wprowadzone za pomocą polecenia cmdlet programu PowerShell są odzwierciedlone w konsoli zarządzania programu DPM.



Wykluczenie woluminu

Serwery programu DPM mogą być zarządzane przez zespół administratorów. Chociaż istnieją wskazówki dotyczące magazynu, które powinny być używane do tworzenia kopii zapasowych, nieprawidłowy wolumin przyznany do programu DPM jako magazyn kopii zapasowych może prowadzić do utraty danych o kluczowym znaczeniu. W związku z tym w przypadku programu DPM 2016 UR4 i nowszych można zapobiec takim scenariuszom, konfigurując te woluminy jako dostępne dla magazynu przy użyciu programu PowerShell.

Na przykład, aby wykluczyć F:\ i C:\MountPoint1, poniżej przedstawiono kroki:

1. Uruchom Set-DPMGlobalProperty polecenia cmdlet:

```
Set-DPMGlobalProperty -DPMStorageVolumeExclusion "F:,C:\MountPoint1"
```

2. Wykonaj ponowne skanowanie magazynu za pomocą interfejsu użytkownika lub użyj polecenia cmdlet

Start-DPMDiskRescan.

Skonfigurowane woluminy i mountpoints są wykluczone.

3. Aby usunąć wykluczenie woluminu, uruchom następujące polecenie cmdlet:

```
Set-DPMGlobalProperty -DPMStorageVolumeExclusion ""
```

Po usunięciu wykluczenia woluminu ponownie Przeskanuj magazyn. Wszystkie woluminy i punkty instalacji, z wyjątkiem woluminów systemowych, są dostępne dla magazynu programu DPM.

Migracja magazynu kopii zapasowych

Gdy wszystkie kopie zapasowe znajdują się w MB, może być konieczne Migrowanie niektórych źródeł danych z jednego woluminu do drugiego. Na przykład scenariusze, w których należy uaktualnić magazyn lub kiedy wolumin jest pełny. Do migracji źródeł danych można użyć programu PowerShell lub interfejsu użytkownika. Szczegóły można znaleźć [w tym wpisie na blogu](#).

Migrowanie źródła danych powinno obejmować wszystkie punkty odzyskiwania w nowoczesnej pamięci masowej. Migrowanie źródeł danych z kopiami zapasowymi na dyskach i woluminach (na przykład uaktualnienia serwera programu DPM, gdy kopie zapasowe dysków nie wygasły) nie są obsługiwane. Migracja jest podobna do modyfikacji grupy ochrony. Podczas migracji nie można wyzwoić zadania ad hoc. Zaplanowane zadania są nadal skonfigurowane. Po zakończeniu migracji wszystkie uruchomione zadania w grupie ochrony zostaną przeniesione.

Alokacja rozmiaru niestandardowego

Program DPM 2016 zużywa cienki magazyn w razie konieczności. Po skonfigurowaniu programu DPM do ochrony obliczany jest rozmiar kopii zapasowej danych. Jeśli kopia zapasowa wielu plików i folderów jest tworzona razem, tak jak w przypadku serwera plików, Obliczanie rozmiaru może trwać długo. W programie DPM można skonfigurować program DPM do akceptowania rozmiaru woluminu jako domyślnego zamiast obliczania rozmiaru każdego pliku. Odpowiedni klucz rejestru to "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft Data Protection Manager\Configuration\DiskStorage" z kluczem "EnableCustomAllocationOnReFSStorage" jako ciąg ustawionym na 1, aby włączyć alokację rozmiaru niestandardowego, ustaw wartość 0. dla domyślnego przydziału rozmiaru w programie DPM.

Nowoczesny magazyn kopii zapasowych (MB) została wprowadzona w programie System Center Data Protection Manager (DPM) 2016, aby dostarczyć 50% oszczędności za magazyn, 3. szybsze kopie zapasowe i wydajny magazyn z obsługą obciążeń. W przypadku programu DPM 2019 wprowadzono dalsze ulepszenia wydajności w programie MB, co spowodowało 50-70% szybsze tworzenie kopii zapasowych w systemie Windows Server 2019.

NOTE

Zalecamy wdrożenie programu DPM 2019 (przy użyciu woluminów warstwowych) w systemie Windows Server 2019 w celu osiągnięcia zwiększonych osiągnięć kopii zapasowych.

- MB jest włączana automatycznie w przypadku uruchomienia co najmniej programu DPM 2016 w systemie Windows Server 2016. Jeśli program DPM jest uruchomiony w wersji systemu Windows Server starszej niż Windows Server 2016, nie używa MB.
- MB zapewnia inteligentny magazyn do krótkoterminowej kopii zapasowej na dysku. MB zapewnia szybszą kopię zapasową dysku, zużywając mniej miejsca na dysku. Bez MB każdego źródła danych wymagane są dwa woluminy, jeden dla początkowej kopii zapasowej, a drugi dla zmian różnicowych.
- Kopie zapasowe MB są przechowywane na dysku systemu plików ReFS. Używa ona klonowania bloków systemu plików ReFS i technologii VHDX. [Dowiedz się więcej](#).

- W przypadku programu DPM 2019 i nowszych można używać woluminów warstwowych dla natywnego magazynu programu DPM, który oferuje 50-70% szybsze kopie zapasowe

NOTE

Program DPM nie obsługuje deduplikacji na dysku ReFS używanym do tworzenia kopii zapasowych MB.

Program DPM 2019 akceptuje woluminy/dyski dla magazynu. Po dodaniu woluminu program DPM sformatuje wolumin do systemu plików ReFS, aby korzystać z nowych funkcji Nowoczesny magazyn kopii zapasowych. Woluminy nie mogą znajdować się na dysku dynamicznym, używaj tylko dysku podstawowego.

Można jednak bezpośrednio przekazać wolumin do programu DPM, ale w razie potrzeby mogą wystąpić problemy z rozszerzeniem woluminu. Dodatkowe woluminy można utworzyć przy użyciu pul magazynów, które mogą być udostępniane w programie DPM i rozszerzane w razie potrzeby. Poniższe sekcje zawierają szczegółowe informacje dotyczące sposobu tworzenia woluminu warstwowego, dodawania woluminu do programu DPM i rozszerzania go później

Konfigurowanie MB z Tiered Storage

W programie DPM 2016 wprowadzono Nowoczesny magazyn kopii zapasowych (MB), co zwiększa wykorzystanie magazynu i wydajność. MB używa systemu ReFS jako bazowego systemu plików. MB zaprojektowano tak, aby korzystało z magazynu hybrydowego, takiego jak magazyn warstwowy. Aby osiągnąć skalę i wydajność żadaną przez MB, zalecamy użycie małego procentu (4% całkowitego magazynu) w ramach programu DPM 2019 jako woluminu warstwowego w połączeniu z dyskiem twardym dla magazynu natywnego programu DPM.

NOTE

- Obsługa warstw jest zalecana w przypadku szybszych kopii zapasowych. Nie jest to jednak wymagane do skonfigurowania magazynu programu DPM.
- Nie można dołączyć lokalnie utworzonych plików VHD (VHDX) i używać ich jako magazynu na fizycznym serwerze programu DPM. Upewnij się, że korzystasz z programu DPM 2019 lub nowszej wersji wdrożonej na maszynie wirtualnej z systemem Windows Server 2016 lub nowszym.

Wykonaj kroki opisane w poniższych procedurach, aby skonfigurować MB za pomocą magazynu warstwowego. Postępuj zgodnie z procedurami przedstawionymi poniżej.

1. Skonfiguruj magazyn programu DPM.

NOTE

Migruj bieżące kopie zapasowe do woluminu tymczasowego przy użyciu [migracji woluminu](#), jeśli chcesz zmodyfikować istniejący magazyn do magazynu warstwowego.

- Utwórz pulę magazynów.
 - Utwórz dysk wirtualny z puli magazynów z ustawionym układem na prosty. Następnie można dodać dodatkowe dyski lub zwiększyć dysk wirtualny.
 - Utwórz woluminy warstwowe/proste na dysku wirtualnym.
2. Dodaj woluminy do programu DPM.
3. Przeprowadź migrację danych z powrotem do nowo utworzonych woluminów przy użyciu migracji woluminu wykonanej w kroku 1.

NOTE

Dotyczy tylko sytuacji, gdy zostały zmigrowane starsze kopie zapasowe w kroku 1.

4. Skonfiguruj magazyn obsługujący obciążenie.

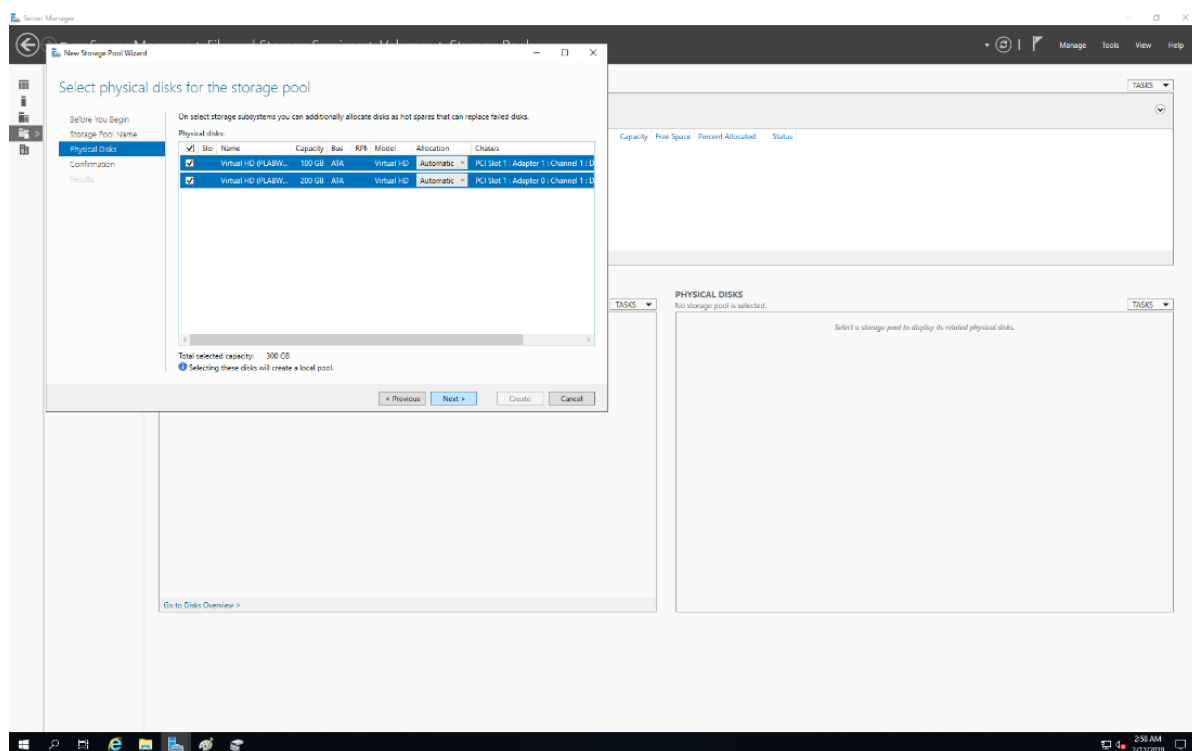
Konfigurowanie magazynu programu DPM

Funkcja miejsca do magazynowania systemu Windows umożliwia łączenie wielu dysków fizycznych w jeden dysk logiczny. Funkcja miejsca do magazynowania korzysta z alokowania elastycznego, która rezerwuje pojemność dysku w miarę przechowywania danych na dysku. Zapewnia łatwy sposób tworzenia magazynu zdefiniowanego programowo przy użyciu zasobów magazynu lokalnego na serwerze.

Konfigurowanie miejsc do magazynowania

Wykonaj następujące kroki::

1. Otwórz **Menedżer serwera**.
2. Kliknij pozycję **usługi plików i magazynowania**.
3. Kliknij pozycję **Pule magazynu**.
4. Wybierz opcję **Nowa pula magazynów z zadań**.
5. Wprowadź nazwę puli magazynów, a następnie kliknij przycisk **dalej**.
6. Dołącz dysk fizyczny do puli magazynów. Jeśli brakuje dysku w puli pierwotnej, możesz dodać go, wybierając opcję **Dodaj dysk fizyczny** z menu rozwijanego **zadania**.



NOTE

Pierwotna Pula jest tworzona domyślnie i jest zasadniczo repozytorium dla dysków, które są dostępne do użycia w tworzonej puli magazynów. Dysk może należeć tylko do jednej puli magazynów.

7. Sprawdź typ nośnika dołączonego dysku. Co najmniej jeden z dysków powinien mieć dysk SSD wymagany

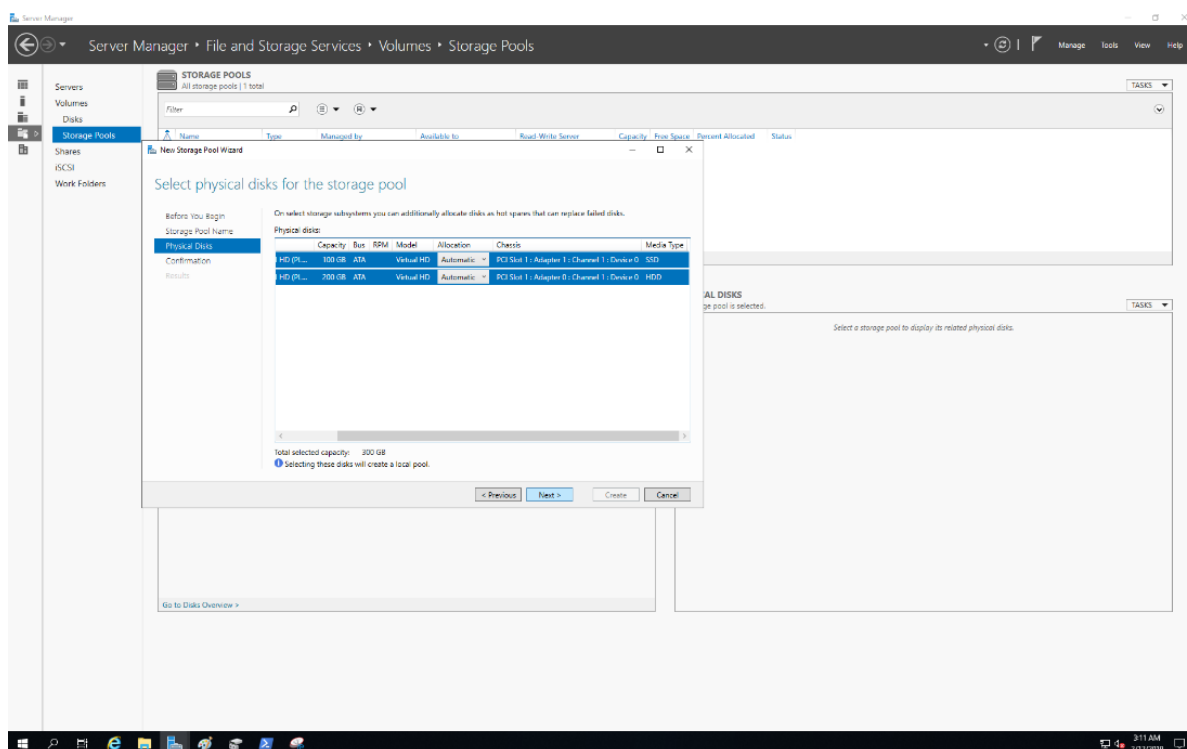
do obsługi warstw dyskóv SSD.

- Dodaj wszystkie dyski, w tym dyskóv SSD do puli magazynóv.
- Dodaj tylko jeden dysk do puli, aby zachować liczbę kolumn na 1. Następnie można dodać dyski odpowiednio do wymagań.

NOTE

- W przypadku dodania wielu dyskóv do puli magazynóv w ramach języka go liczba dyskóv jest przechowywana jako liczba kolumn. Po dodaniu większej liczby dyskóv może to być tylko wielokrotność liczby kolumn.
- W przypadku programu DPM uruchomionego na maszynach wirtualnych udostępnienie wirtualnych dyskóv twardych używać miejsca z fizycznych dyskóv SSD & HDD z komputera hosta do maszyny wirtualnej i użycie ich jako magazynu warstwowego, jak wyjaśniono powyżej.

Na poniższej ilustracji przedstawiono sprawdzanie typu dysku:



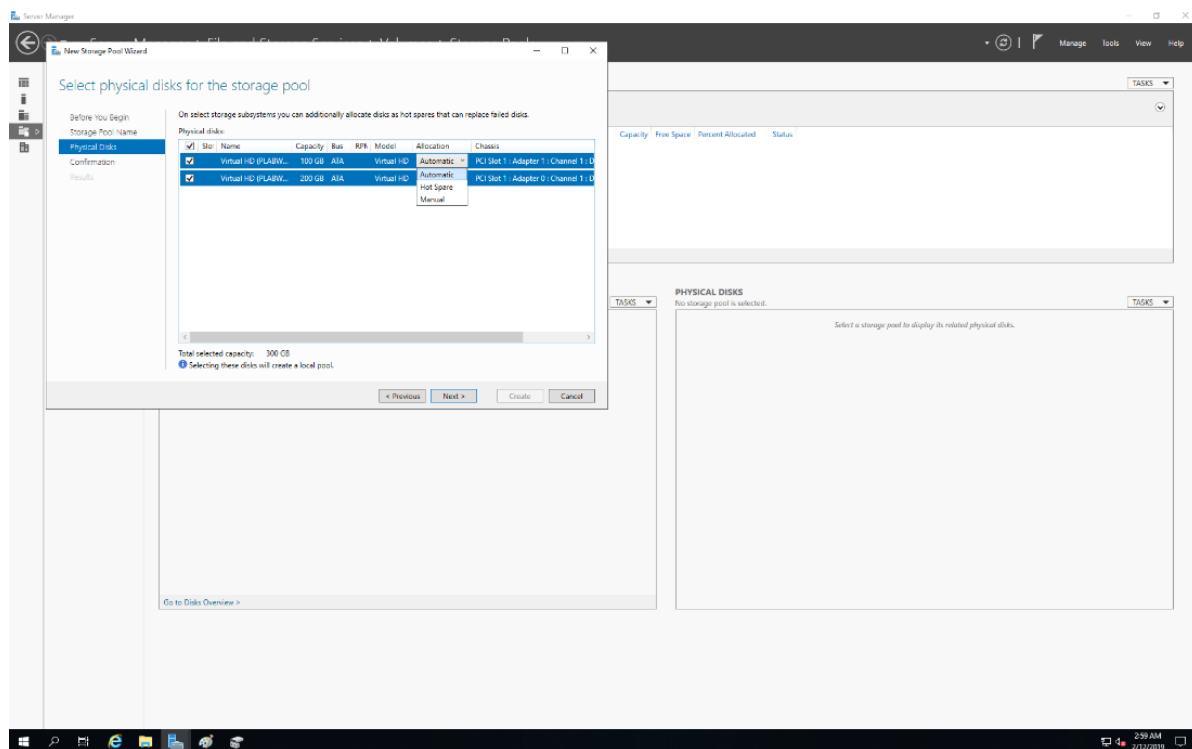
8. Jeśli nie można prawidłowo rozpoznać typu nośnika dla dysku twarde lub dysk SSD, użyj następującego polecenia:

`Set-DiskFizyczny-unikatowy <ciąg unikatowy> -MediaType < dysk twardy | > SSD`

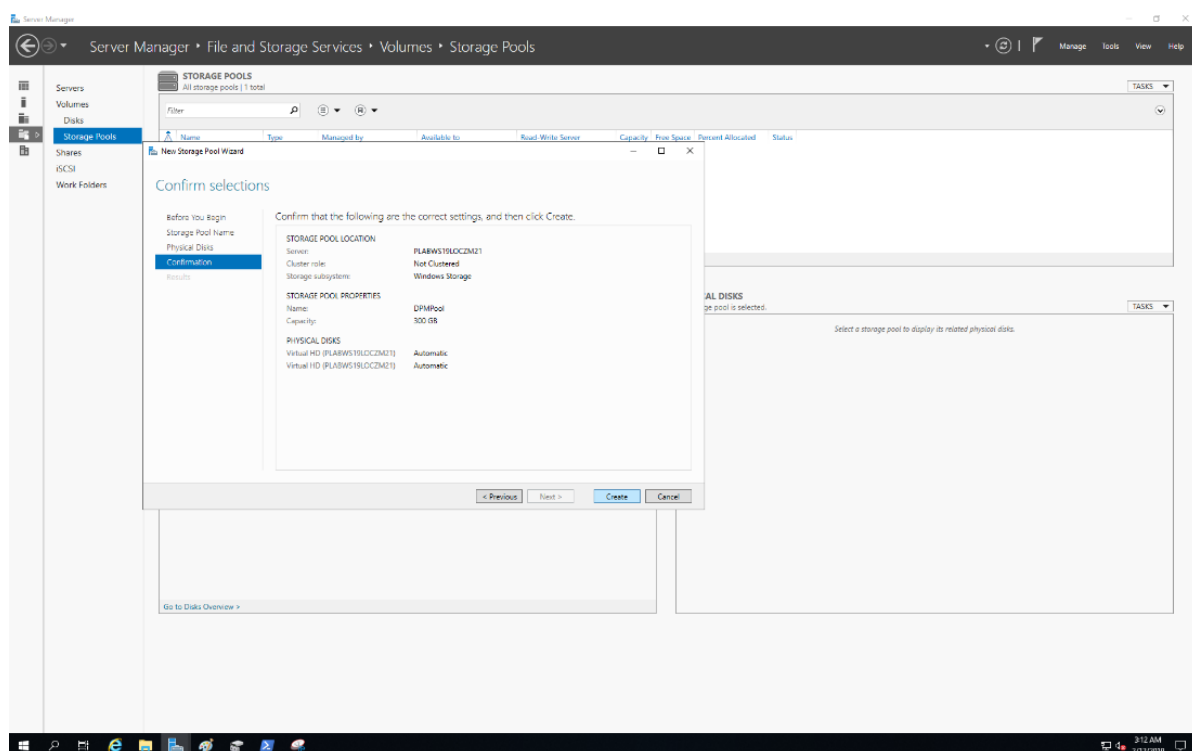
```
PS C:\> Set-PhysicalDisk -UniqueId '{0354754c-2385-11e9-b4d8-806e6f6e6963}' -MediaType HDD
PS C:\> Set-PhysicalDisk -UniqueId '{ba87dacb-2eb3-11e9-b4d9-806e6f6e6963}' -MediaType HDD
PS C:\> Set-PhysicalDisk -UniqueId '{0354754d-2385-11e9-b4d8-806e6f6e6963}' -MediaType SSD
PS C:\> Get-PhysicalDisk | Select-Object UniqueID,Size,MediaType

UniqueID                               Size  MediaType
-----
{0354754c-2385-11e9-b4d8-806e6f6e6963} 214748364800 HDD
{0354754d-2385-11e9-b4d8-806e6f6e6963} 107374182400 SSD
{ba87dacb-2eb3-11e9-b4d9-806e6f6e6963} 42949672960  HDD
```

9. Dla każdego z tych dyskóv Ustaw alokację jako **automatyczną**.



10. Sprawdź wprowadzone opcje, a następnie kliknij przycisk **Utwórz**, aby utworzyć nową pulę magazynów.



Po pomyślnym utworzeniu puli magazynów nowo utworzona Pula magazynów zostanie wyświetlona w obszarze **Pula magazynów**. **Dysk fizyczny** wyświetla dyski, które znajdują się w wybranej puli.

Wyłącz pamięć podręczną zapisu

Wyłącz pamięć podręczną zapisu, aby wyłączyć automatyczne buforowanie na poziomie puli magazynu (wymagana tylko dla magazynu warstwowego).

W tym celu przejdź do programu PowerShell i wykonaj następujące polecenia:

```
Set-StoragePool -FriendlyName <String> [-WriteCacheSizeDefault <UInt64>]
```

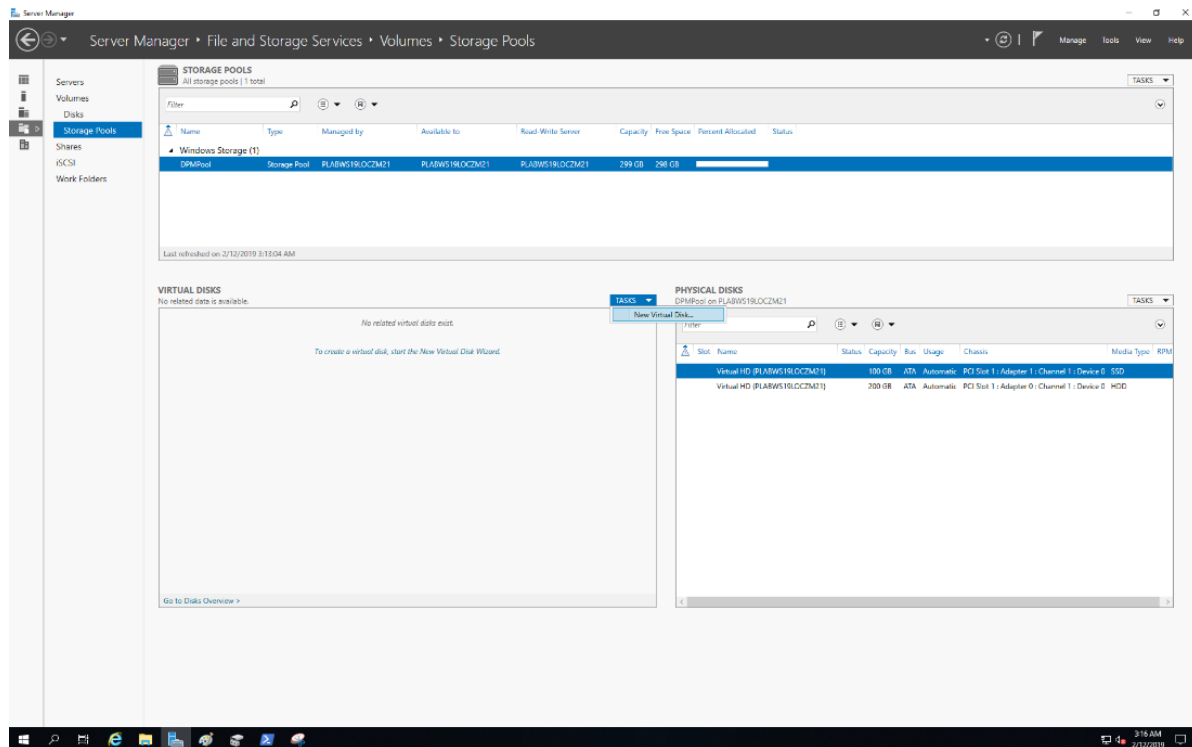
Wybierz opcję WriteCacheSizeDefault wartość 0.

```
PS C:\>  
PS C:\> Set-StoragePool -FriendlyName DMPool -WriteCacheSizeDefault 0  
PS C:\>
```

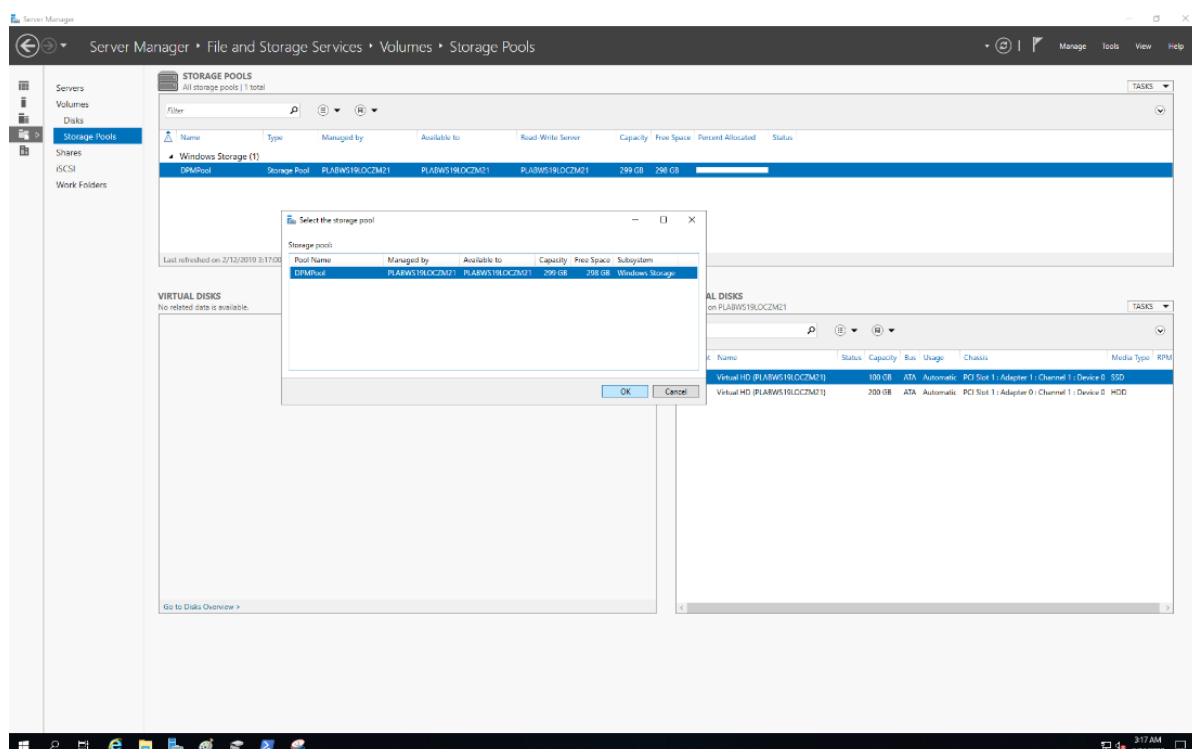
Tworzenie dysków wirtualnych

Wykonaj następujące kroki:

1. W okienku **dysk wirtualny** wybierz pozycję **nowy dysk wirtualny** z menu rozwijanego **zadania**.



2. Wybierz pulę magazynów, z której chcesz utworzyć dysk wirtualny.

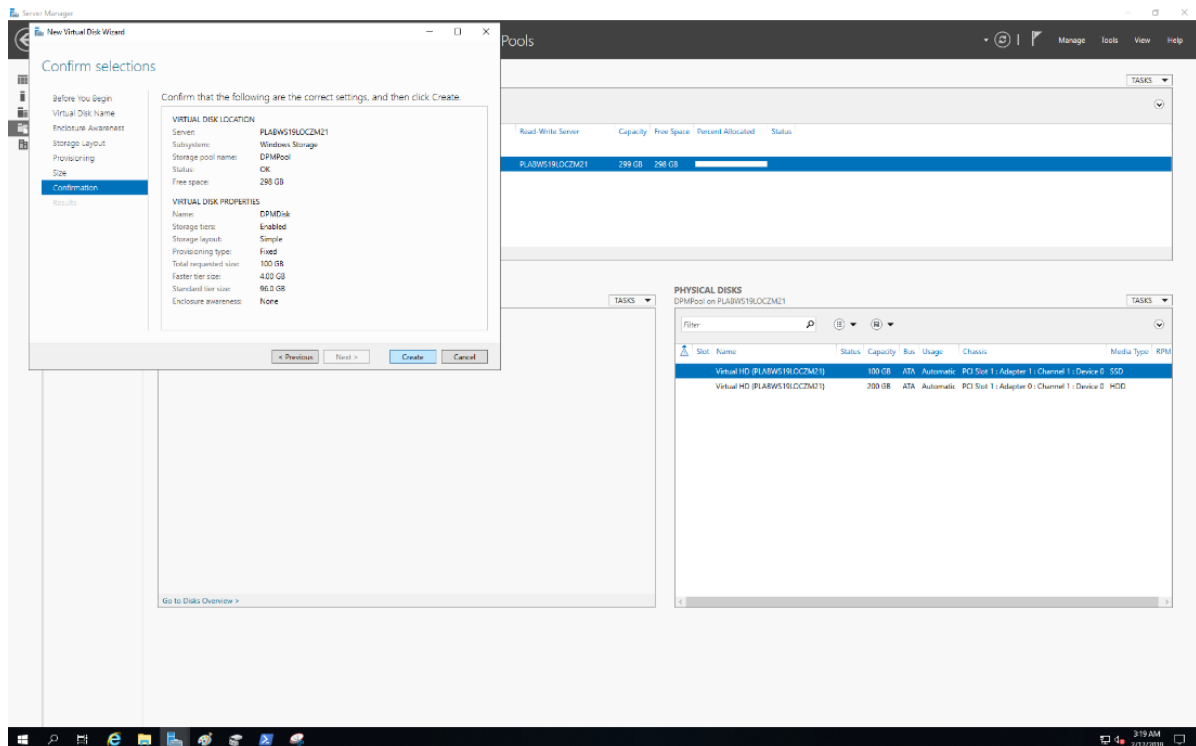


3. Podaj nazwę dysku wirtualnego.

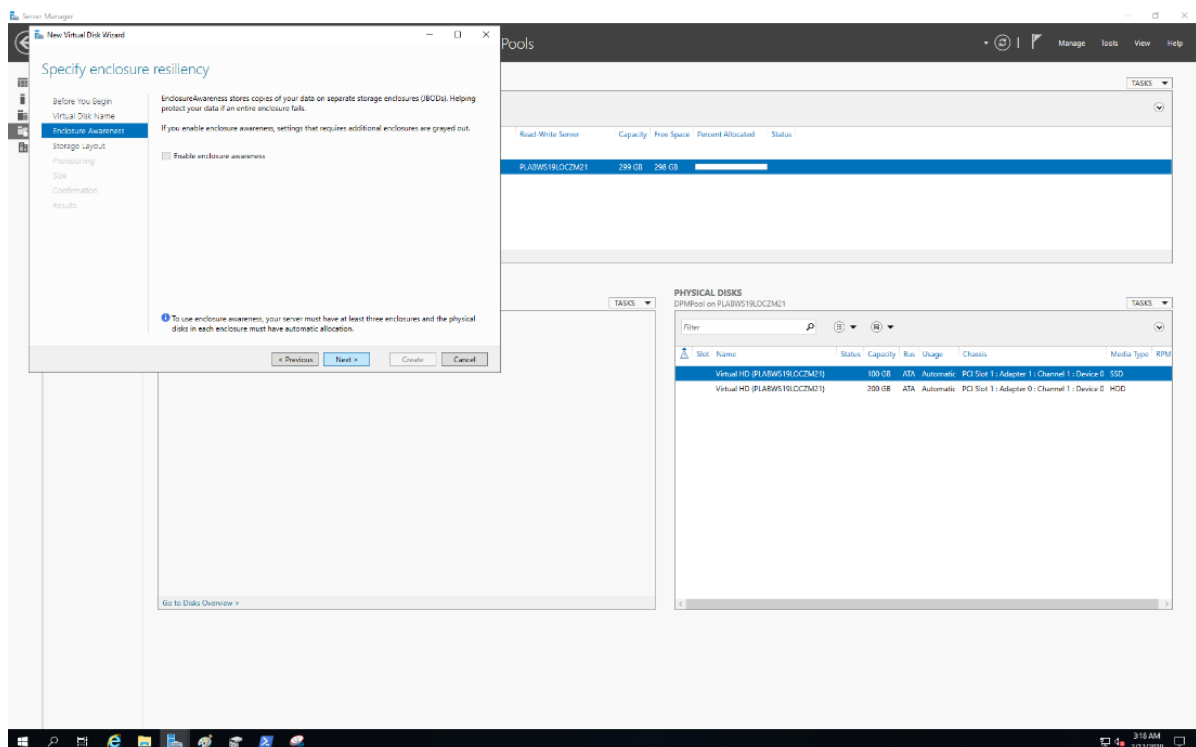
4. Wybierz pozycję **Utwórz warstwy magazynowania na tym dysku wirtualnym** , aby utworzyć magazyn warstwowy.

NOTE

Tiered Storage jest możliwe tylko wtedy, gdy pula magazynów zawiera kombinację dysków SSD i dysków twardych.

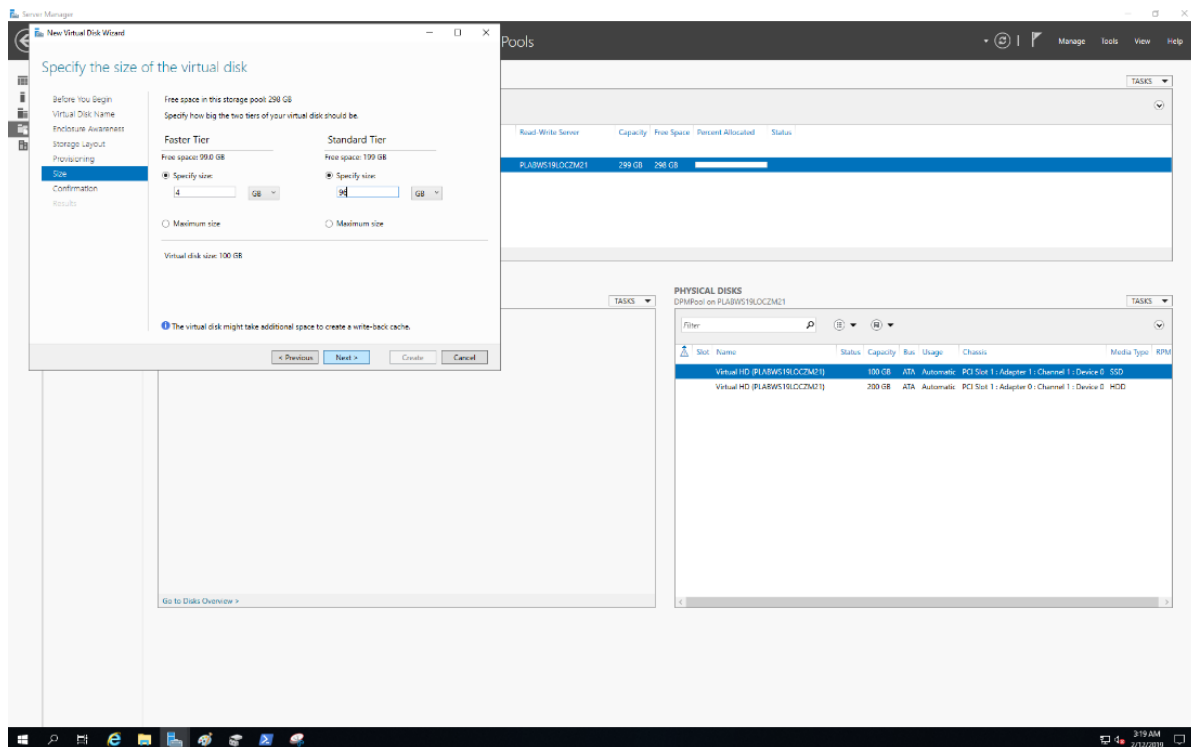


5. Kliknij przycisk **dalej** i wybierz pozycję **Włącz rozpoznawanie obudowy (jeśli jest to wymagane)** .

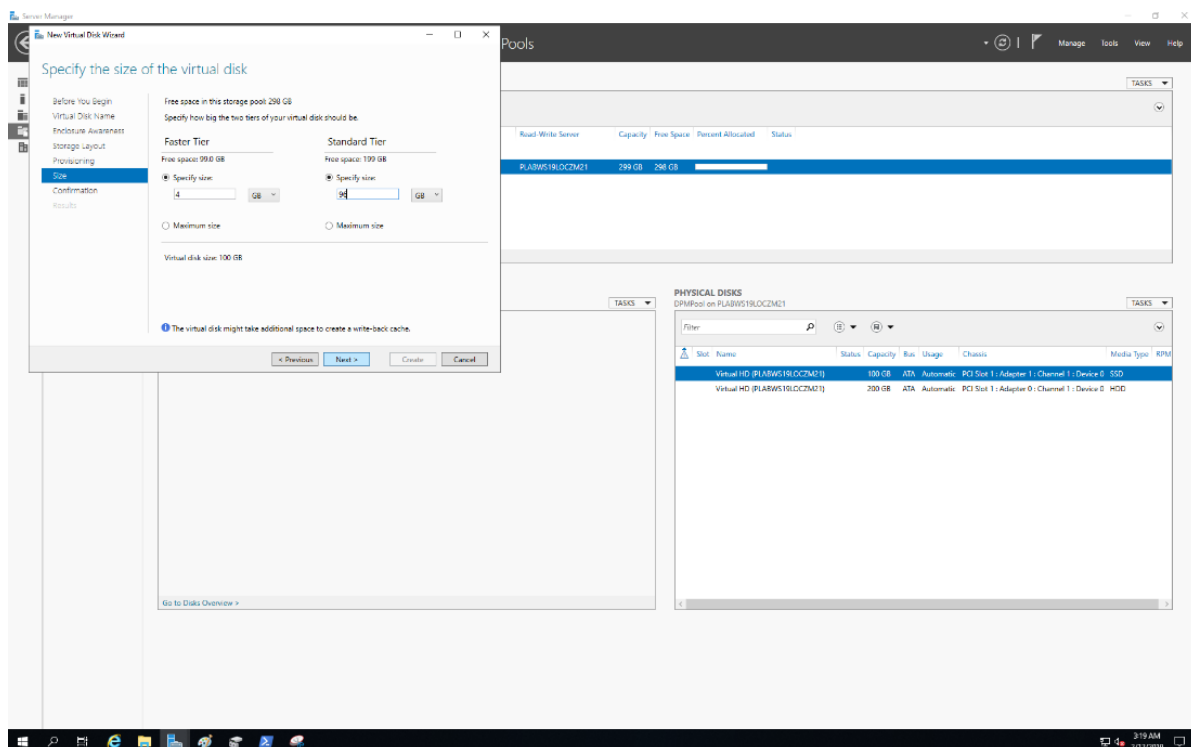


6. Wybierz pozycję **Układ prosty** i kliknij przycisk **dalej**.
7. Alokacja **stała** jest opcją domyślną. Kliknij przycisk **Dalej**.
8. Podaj rozmiar **szybszej** warstwy i **warstwy Standardowa**. **Szybsza warstwa** odpowiada dyskom SSD i

warstwom standardowym odpowiadającym dysków twardym. Rozmiar warstwy szybszej powinien wynosić 4% rozmiaru warstwy Standard (na przykład. Jeśli łączny wymóg wynosi 100 GB — Jeśli dysk twardy ma 96 GB, SDD powinien mieć wartość 4 GB. Kliknij przycisk **Dalej**.



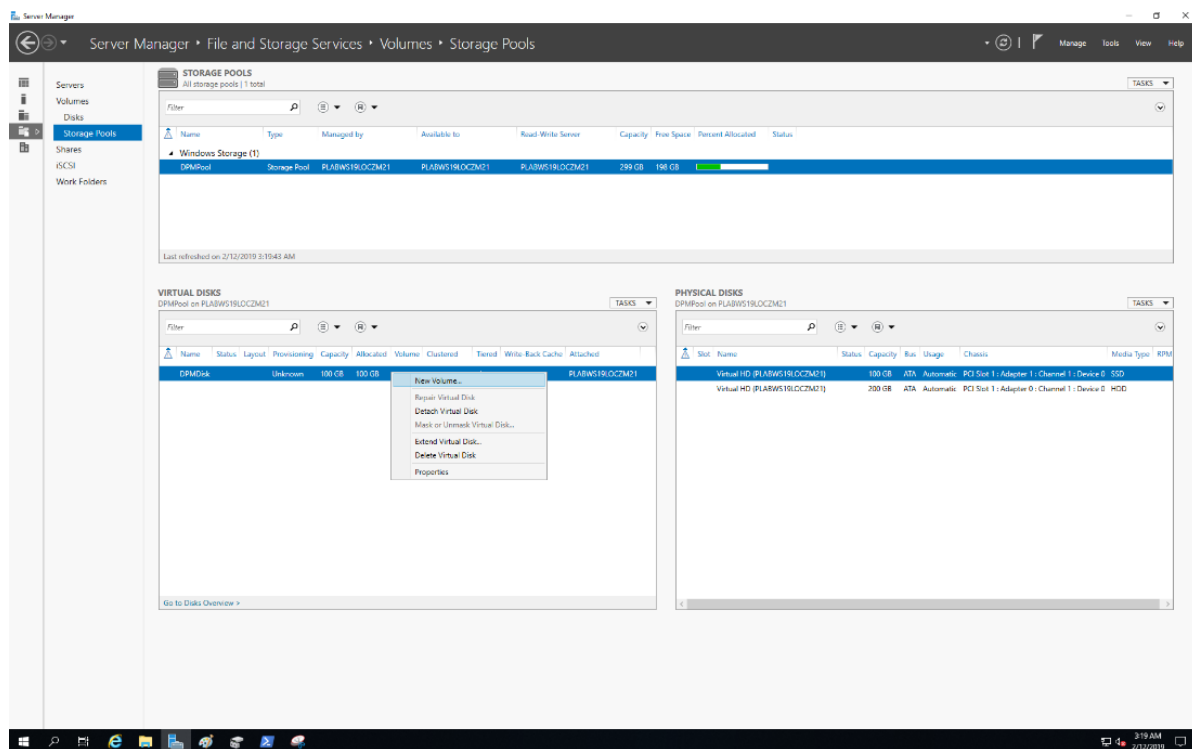
9. Potwierdź konfigurację i kliknij przycisk **Utwórz**.



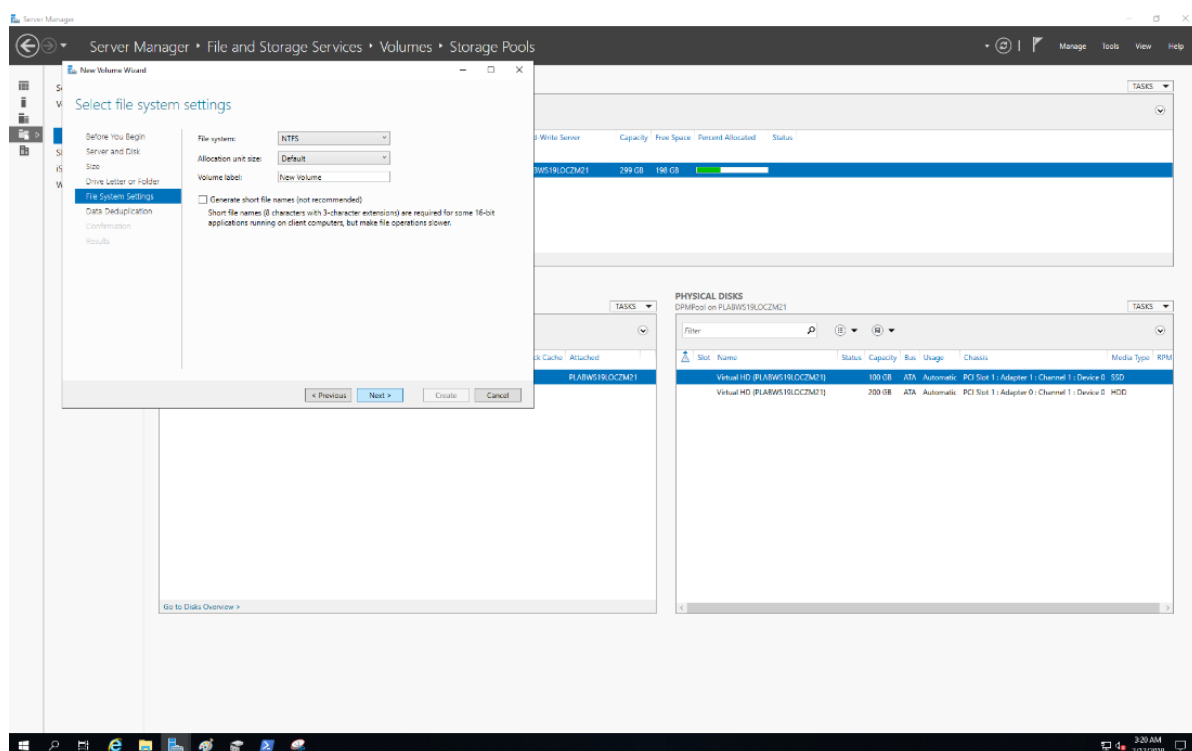
Tworzenie woluminu

Wykonaj następujące kroki:

1. Wybierz dysk wirtualny, który został utworzony, i uruchom **Kreatora nowego woluminu**.



2. W **Kreatorze nowego woluminu** kliknij przycisk **dalej**, Przypisz literę dysku i określ rozmiar.



3. Kliknij przycisk **Zakończ**, aby utworzyć nowy wolumin.
4. Sformatuj utworzony wolumin z konsoli **Zarządzanie dyskami** na system plików ReFS.

Wyłącz automatyczne buforowanie na poziomie systemu plików

1. Przejdź do programu PowerShell.
2. Użyj następującego polecenia:

```
fsutil behavior disableWriteAutoTiering
```

Sposób użycia: Fsutil behavior set disableWriteAutoTiering <nazwa ścieżki woluminu> <1 | 0 >:

0 - Enable write auto tiering on the given volume (default)

1 - Disable write auto tiering on the given volume

Przykład: Fsutil behavior set disableWriteAutoTiering C: 1

```
PS C:\>
PS C:\> fsutil behavior set disableWriteAutoTiering E: 1
The volume state is: 1 (write auto tiering is disabled).
PS C:\>
```

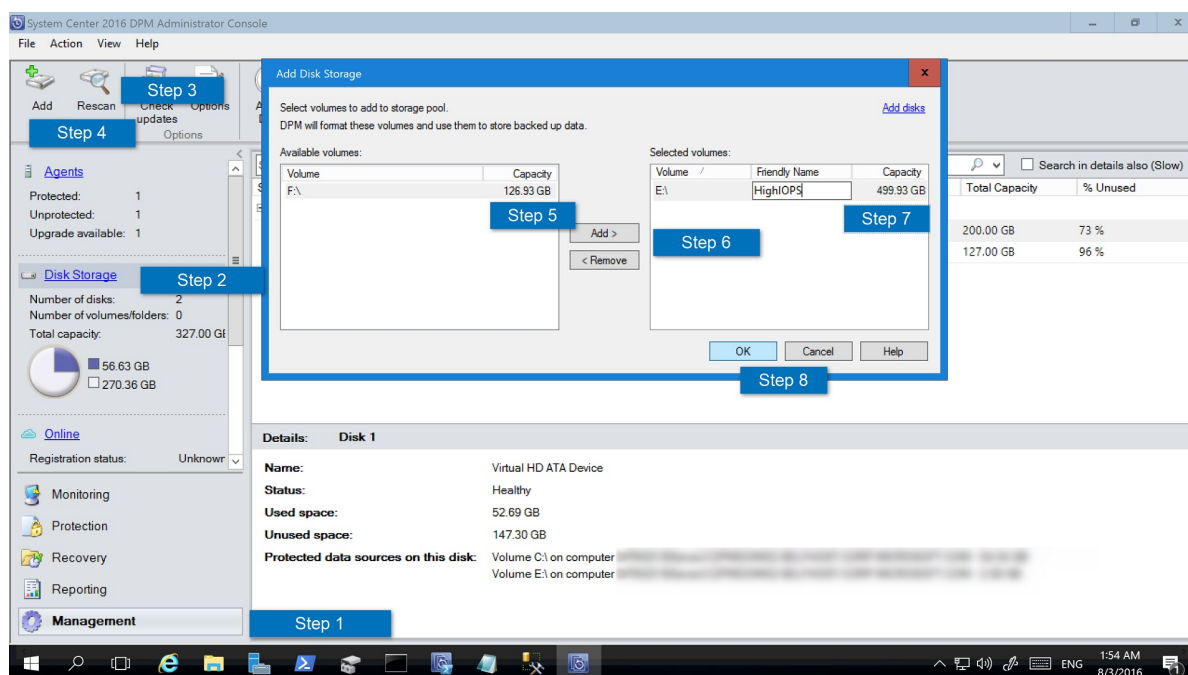
Należy pamiętać, że ten krok można pominąć, jeśli jest dostępny więcej niż 10% dysków SSD. Tę możliwość można wyłączyć później, jeśli występuje spadek wydajności w zakresie szybkości wykonywania kopii zapasowych.

Teraz Dodaj nowo utworzone woluminy do magazynu programu DPM, korzystając z procedury opisanej poniżej.

Dodawanie woluminów do magazynu programu DPM

Wykonaj następujące kroki:

1. W konsoli zarządzania programu DPM > **Disk Storage** kliknij pozycję **Skanuj** ponownie.
2. W obszarze **dodaj Disk Storage** kliknij pozycję **Dodaj**.
3. Po dodaniu woluminów można nadać im przyjazną nazwę.
4. Kliknij przycisk **OK**, aby sformatować woluminy do systemu plików ReFS, aby program DPM mógł ich używać jako MB.



Migrowanie danych do nowo utworzonych woluminów

W przypadku uaktualnienia istniejącego magazynu do magazynu warstwowego można migrować dane za pomocą migracji woluminu. Do migracji źródeł danych można użyć programu PowerShell lub interfejsu użytkownika. [Dowiedz się więcej](#).

Migracja źródła danych powinna obejmować wszystkie punkty odzyskiwania w nowoczesnej pamięci masowej.

NOTE

- Migracja źródeł danych przy użyciu kopii zapasowych na dyskach i woluminach (na przykład uaktualnienia serwera DPM, gdy kopie zapasowe dysku nie wygasły) nie są obsługiwane.
- Migracja jest podobna do modyfikacji grupy ochrony. Podczas migracji nie można wyzwoić zadania ad hoc. Zaplanowane zadania są nadal skonfigurowane. Po zakończeniu migracji bieżące zadania w grupie ochrony zostaną przeniesione.

Konfigurowanie magazynu obsługującego obciążenie

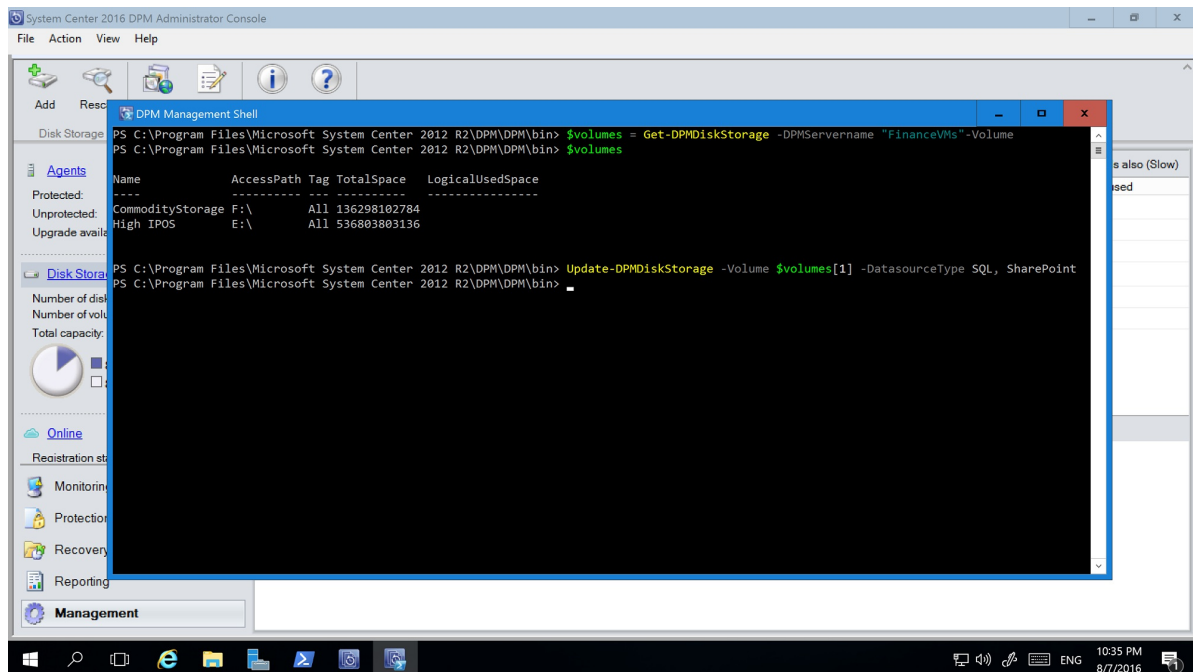
Korzystając z magazynu obsługującego obciążenie, można wybierać woluminy w celu preferencyjnego przechowywania określonych obciążeń. Na przykład drogie woluminy obsługujące dużą liczbę IOPS można skonfigurować do przechowywania obciążeń wymagających częstych kopii zapasowych, takich jak SQL Server z dziennikami transakcji. W przypadku obciążeń, dla których kopie zapasowe są tworzone rzadziej, takich jak maszyny wirtualne, można utworzyć kopię zapasową na woluminach o niskim koszcie.

Magazyn obsługujący obciążenia można skonfigurować przy użyciu poleceń cmdlet programu Windows PowerShell.

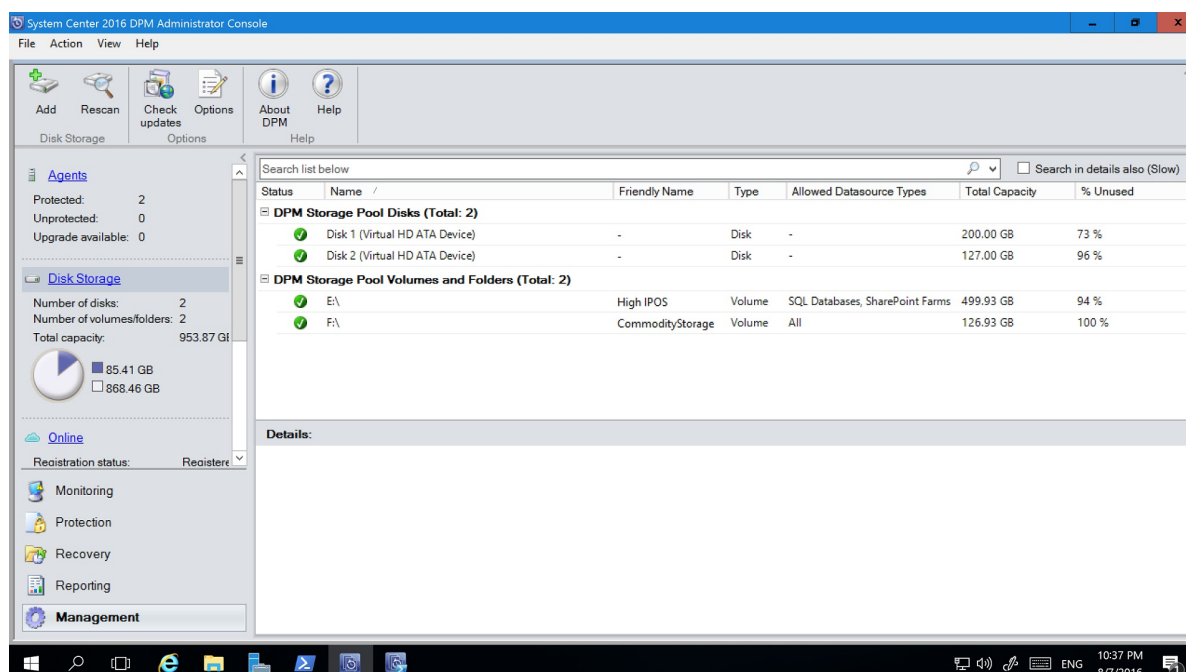
Aktualizowanie właściwości woluminu

1. Uruchom **aktualizację Update-DPMDiskStorage**, aby zaktualizować właściwości woluminu w puli magazynów na serwerze programu DPM. Składnia to **zestaw parametrów: wolumin**.
2. Uruchom polecenie cmdlet z tymi parametrami.

```
Update-DPMDiskStorage [-Volume] <Volume> [[-FriendlyName] <String> ] [[-DatasourceType] <VolumeTag[]> ]  
[-Confirm] [-WhatIf] [ <CommonParameters>]
```



Zmiany wprowadzone za pomocą polecenia cmdlet programu PowerShell są odzwierciedlone w konsoli zarządzania programu DPM.



Wykluczenie woluminu

Serwery programu DPM mogą być zarządzane przez zespół administratorów. Chociaż istnieją wskazówki dotyczące magazynu, które powinny być używane do tworzenia kopii zapasowych, nieprawidłowy wolumin przyznany do programu DPM jako magazyn kopii zapasowych może prowadzić do utraty danych o kluczowym znaczeniu. W związku z tym w przypadku programu DPM 2016 UR4 i nowszych można zapobiec takim scenariuszom, konfigurując te woluminy jako *dostępne* dla magazynu przy użyciu programu PowerShell.

Na przykład, aby wykluczyć F:\ i C:\MountPoint1, wykonaj następujące kroki:

1. Uruchom Set-DPMGlobalProperty polecenia cmdlet:

```
Set-DPMGlobalProperty -DPMStorageVolumeExclusion "F:,C:\MountPoint1"
```

2. Wykonaj ponowne skanowanie magazynu za pomocą interfejsu użytkownika lub użyj polecenia cmdlet Start-DPMDiskRescan.

Skonfigurowane woluminy i mountpoints są wykluczone.

3. Aby usunąć wykluczenie woluminu, uruchom następujące polecenie cmdlet:

```
Set-DPMGlobalProperty -DPMStorageVolumeExclusion ""
```

Po usunięciu wykluczenia woluminu ponownie Przeskanuj magazyn. Wszystkie woluminy i punkty instalacji, z wyjątkiem woluminów systemowych, są dostępne dla magazynu programu DPM.

Alokacja rozmiaru niestandardowego

Program DPM 2019 zużywa cienki magazyn w razie konieczności. Po skonfigurowaniu programu DPM do ochrony obliczany jest rozmiar kopii zapasowej danych. Jeśli kopia zapasowa wielu plików i folderów jest tworzona razem, tak jak w przypadku serwera plików, Obliczanie rozmiaru może trwać długo.

W przypadku programu DPM 2016 i nowszych można skonfigurować program DPM do akceptowania rozmiaru woluminu jako domyślnego zamiast obliczania rozmiaru każdego pliku. Odpowiedni klucz rejestru jest *HKEY_LOCAL_MACHINE \Software\microsoft\microsoft ochrony danych Manager\Configuration\DiskStorage* z kluczem, *EnableCustomAllocationOnReFSStorage* jako ciąg ustawionym na 1, aby włączyć alokację rozmiaru

niestandardowego, ustaw wartość 0 dla domyślnego przydziału rozmiaru w programie DPM.

Deduplikacja magazynu programu DPM

10.01.2020 • 34 minutes to read

Program System Center Data Protection Manager (DPM) może korzystać z deduplikacji danych.

Deduplikacja danych (Deduplikacja) odnajduje i usuwa zduplikowane dane w woluminie, a jednocześnie zapewnia prawidłowe i kompletne dane. Przeczytaj więcej na temat [planowania deduplikacji](#).

- Deduplikacja redukuje zużycie magazynu i chociaż ilość redundancji dla zestawu danych zależy od obciążenia i typu danych, zwykle po zastosowaniu deduplikacji da się osiągnąć duże oszczędności na danych kopii zapasowej.
- Redundancja danych można być jeszcze bardziej ograniczona za pomocą deduplikacji podczas wspólnego przetwarzania danych kopii zapasowej podobnych typów i obciążeń.
- Deduplikacja jest przeznaczona do instalowania na podstawowych woluminach danych bez dodatkowego dedykowanego sprzętu, dzięki czemu nie ma to wpływu na podstawowe obciążenie na serwerze. Ustawienia domyślne nie narzucają niczego, ponieważ dane mogą być przechowywane przez pięć dni przed rozpoczęciem przetwarzania danego pliku. Domyślny minimalny rozmiar pliku wynosi 32 KB. Implementacja została zaprojektowana z myślą o małym użyciu pamięci i procesora CPU.
- Deduplikację można zaimplementować dla następujących obciążeń:
 - Ogólne udziały plików: publikowanie i udostępnianie zawartości grupy, foldery macierzyste użytkownika i pliki /offline/przekierowanie folderu
 - Udziały wdrożenia oprogramowania: pliki binarne, obrazy i aktualizacje oprogramowania.
 - Biblioteki wirtualnego dysku twardego: magazyn plików wirtualnego dysku twardego (VHD) na potrzeby aprowizacji funkcji hypervisor
 - Wdrożenia infrastruktury VDI (tylko system Windows Server 2012 R2): wdrożenia infrastruktury pulpitu wirtualnego (VDI) korzystające z funkcji Hyper-V
 - Zwirtualizowana kopia zapasowa: rozwiązania do tworzenia kopii zapasowej (takie jak program DPM działający na maszynie wirtualnej z funkcją Hyper-V), które zapisują dane kopii zapasowej do plików VHD/VHDX na serwerze plików systemu Windows.

Program DPM i deduplikacja

Korzystanie z deduplikacji w programie DPM może ułatwić uzyskiwanie dużych oszczędności. Ilość miejsca oszczędzanego przez funkcję deduplikacji podczas optymalizacji danych kopii zapasowej programu DPM zależy od typu danych uwzględnianych w tworzonej kopii zapasowej. Na przykład tworzenie kopii zapasowej zaszyfrowanego serwera baz danych może spowodować minimalne oszczędności, ponieważ wszystkie zduplikowane dane są ukrywane podczas procesu szyfrowania. Natomiast wykonanie kopii zapasowej dużego wdrożenia infrastruktury pulpitu wirtualnego (VDI) może spowodować uzyskanie bardzo dużych oszczędności, rzędu 70-90+%, ponieważ przeważnie ilość danych duplikowana między środowiskami pulpitu wirtualnego jest duża. W konfiguracji opisanej w tym temacie firma Microsoft uruchomiła wiele obciążeń testowych i uzyskała oszczędności w zakresie od 50% do 90%.

Aby użyć deduplikacji dla magazynu programu DPM, program DPM powinien działać na maszynie wirtualnej z funkcją Hyper-V i przechowywać dane kopii zapasowej w plikach VHD w folderach udostępnionych z włączoną deduplikacją danych.

Zalecane wdrożenie

W celu wdrożenia programu DPM jako maszyny wirtualnej tworzącej kopię zapasową danych na deduplikowanym woluminie zaleca się użycie następującej topologii wdrażania:

- Program DPM działający na maszynie wirtualnej w klastrze hosta funkcji Hyper-V.
- Magazyn programu DPM korzystający z plików VHD/VHDX przechowywanych w udziale SMB 3.0 na serwerze plików.
- W tym przykładzie skonfigurowaliśmy serwer plików jako skalowany- serwer plików (SOFS) wdrożony przy użyciu woluminów magazynu skonfigurowanych z poziomu pul miejsc do magazynowania z użyciem bezpośrednio połączonych dysków SAS. Należy zwrócić uwagę, że to wdrożenie zapewnia wydajność w odpowiedniej skali.

Należy pamiętać o następujących kwestiach:

- To wdrożenie jest obsługiwane w przypadku programu DPM 2012 R2 lub nowszego oraz dla wszystkich danych obciążenia, których kopię zapasową można utworzyć przy użyciu programu DPM 2012 R2 lub nowszego.
- Wszystkie węzły serwera plików systemu Windows, na których znajdują się wirtualne dyski twarde programu DPM i na którym zostanie włączona funkcja deduplikacji, muszą mieć uruchomiony system Windows Server 2012 R2 z [pakietem zbiorczym aktualizacji listopad 2014](#) lub nowszym.
- Firma Microsoft udostępni ogólne zalecenia i instrukcje dotyczące wdrażania scenariusza. W każdym przykładzie odwołującym się do określonego sprzętu jako punkt odniesienia używany jest sprzęt wdrożony w systemie Microsoft Cloud Platform System (CPS).
- W tym scenariuszu zdalne udziały SMB 3.0 są używane do przechowywania danych kopii zapasowej, dlatego podstawowe wymagania sprzętowe skupiają się wokół węzłów serwera plików, a nie węzłów funkcji Hyper-V. Następująca konfiguracja sprzętu jest używana w systemie CPS na potrzeby magazynu kopii zapasowej i produkcyjnego. Należy zwrócić uwagę na to, że ogólne elementy sprzętu są używane na potrzeby magazynów kopii zapasowej oraz produkcyjnego, natomiast liczba dysków wymieniona na liście dla obudów dysków na liście dotyczy tylko magazynów kopii zapasowej.
 - Klaster serwera plików skalowalny w poziomie z 4 węzłami
 - Konfiguracja każdego węzła
 - 2 procesory CPU Intel(R) Xeon(R) E5-2650 0, 2,00 GHz, 2001 MHz, 8 rdzeni, 16 procesorów logicznych
 - 128 GB pamięci RDIMM, 1333 MHz
 - Połączenia magazynu: 2 porty SAS, 1 port 10 GbE iWarp/RDMA
 - 4 obudowy dysku JBOD
 - 18 dysków w każdej obudowie JBOD — 16 dysków twardych o pojemności 4 TB + 2 dyski SSD o pojemności 800 GB
 - Podwójna ścieżka do każdego dysku - zasady równoważenia obciążenia wielościeżkowego we/wy ustawione tylko na pracę w trybie failover
 - Dyski SSD skonfigurowane pod kątem pamięci podręcznej z zapisem zwrotnym (WBC), a pozostałe dyski do dedykowanych napędów dziennika

Konfigurowanie woluminów deduplikacji

Zastanówmy się, jak duże powinny być woluminy, aby mogły obsługiwać deduplikowane pliki VHDX zawierające dane programu DPM. W systemie CPS utworzyliśmy woluminy o rozmiarze 7,2 TB każdy. Optymalny rozmiar woluminu zależy głównie od zakresu i częstotliwości zmian danych w tym woluminie oraz od wielkości przepustowości dostępu do danych w podsystemie magazynu dysku. Należy pamiętać, że jeśli przetwarzanie deduplikacji przebiega wolniej niż wprowadzanie dziennych zmian danych (liczba zmian), wielkość oszczędności będzie się zmniejszać do momentu ukończenia przetwarzania. Aby uzyskać szczegółowe informacje, zobacz [Ustalanie rozmiaru woluminów na potrzeby deduplikacji danych](#). W przypadku woluminów deduplikacji zaleca się korzystanie z następujących zasad ogólnych:

- W celu uzyskania odporności i zwiększonego wykorzystania dysku należy używać miejsc do magazynowania z opcją parzystości i wykrywaniem obudów.
- Aby funkcja deduplikacji plików rozrzedzonych działa lepiej, należy sformatować system NTFS przy użyciu jednostek alokacji 64 KB i dużych segmentów rekordów plików.
- W powyższej konfiguracji zalecany rozmiar woluminu to 7,2 TB, a woluminy zostaną skonfigurowane w następujący sposób:
 - Wykrywanie obudów, podwójna parzystość, 7,2 TB + 1 GB pamięci podręcznej z zapisem zwrotnym
 - ResiliencySettingName == Parzystość
 - PhysicalDiskRedundancy == 2
 - NumberOfColumns == 7
 - Interleave == 256 KB (Wydajność podwójnej parzystości przy przepływie 64 KB jest znacznie niższa niż przy domyślnym przepływie wynoszącym 256 KB)
 - IsEnclosureAware == \$true
 - AllocationUnitSize=64KB
 - Usługa replikacji dużych plików

Skonfiguruj nowy wirtualny dysk w określonej puli magazynów w następujący sposób:

```
New-VirtualDisk -Size 7.2TB -PhysicalDiskRedundancy 2 -ResiliencySettingName Parity -  
StoragePoolFriendlyName BackupPool -FriendlyName BackupStorage -NumberOfColumns 7 -  
IsEnclosureAware $true
```

- Każdy z woluminów należy sformatować jako:

```
Format-Volume -Partition <volume> -FileSystem NTFS -AllocationUnitSize 64KB -UseLargeFRS -Force
```

Następnie we wdrożeniu systemu CPS są one konfigurowane jako pliki CSV.

- Na tych woluminach program DPM będzie przechowywać serię plików VHDX zawierających dane kopii zapasowej. Po sformatowaniu woluminu włącz jego deduplikację w następujący sposób:

```
Enable-DedupVolume -Volume <volume> -UsageType HyperV  
Set-DedupVolume -Volume <volume> -MinimumFileAgeDays 0 -OptimizePartialFiles:$false
```

To polecenie umożliwia również modyfikowanie następujących ustawień deduplikacji na poziomie woluminu:

- Ustaw parametr **UsageType** na **HyperV**: spowoduje to przetwarzanie deduplikacji otwartych plików, które jest wymagane, ponieważ pliki VHDX użyte w magazynie kopii zapasowej

programu DPM pozostają otwarte, jeśli w programie DPM zostanie uruchomiona odpowiednia maszyna wirtualna.

- Wyłącz parametr `PartialFileOptimization`: spowoduje to deduplikację w celu zoptymalizowania wszystkich sekcji otwartego pliku, a nie skanowanie w poszukiwaniu zmienionych sekcji o minimalnym wieku.
- Ustaw parametr `MinFileAgeDays` na 0: wyłączenie parametru `PartialFileOptimization` spowoduje zmianę zachowania parametru `MinFileAgeDays` — podczas deduplikacji będą brane pod uwagę tylko pliki, które nie zostały zmienione w ciągu wybranej liczby dni. Ponieważ chcemy, aby podczas deduplikacji przetwarzanie danych kopii zapasowej wszystkich plików VHDX programu DPM rozpoczęło się bez opóźnień, musimy ustawić parametr `MinFileAgeDays` na wartość 0.

Aby uzyskać więcej informacji na temat konfigurowania deduplikacji, zobacz [Instalowanie i konfigurowanie duplikacji danych](#).

Konfigurowanie magazynu programu DPM

Aby uniknąć problemów z fragmentacją i utrzymać wydajność, magazyn programu DPM jest przydzielany przy użyciu plików VHDX znajdujących się na deduplikowanym woluminie. Na każdym woluminie tworzonych jest 10 dynamicznych plików VHDX o rozmiarze 1 TB każdy, które są następnie dołączane do programu DPM. Należy pamiętać, że nadmiarowe inicjowanie obsługi administracyjnej magazynu o wielkości 3 TB jest przeprowadzane w celu skorzystania z oszczędności pojemności magazynu uzyskanych dzięki funkcji deduplikacji. Ze względu na to, że funkcja deduplikacji powoduje uzyskanie dodatkowych oszczędności związanych z magazynem, na tych woluminach można utworzyć nowe pliki VHDX w celu użycia zaoszczędzonego miejsca. Serwer programu DPM został przetestowany z maksymalnie dołączonymi do niego 30 plikami VHDX.

1. Uruchom następujące polecenie, aby utworzyć wirtualne dyski twarde, które zostaną później dodane do serwera programu DPM:

```
New-SCVirtualDiskDrive -Dynamic -SCSI -Bus $Bus -LUN $Lun -JobGroup $JobGroupId -VirtualHardDiskSizeMB 1048576 -Path $Using:Path -FileName <VHDName>
```

2. Następnie dodaj utworzone wirtualne dyski twarde do serwera programu DPM w następujący sposób:

```
Import-Module "DataProtectionManager"
Set-StorageSetting -NewDiskPolicy OnlineAll
$dpmdisks = @()
$dpmdisks = Get-DPMDisk -DPMServerName $env:computername | ? {$_.CanAddToStoragePool -eq $true -and $_.IsInStoragePool -eq $false -and $_.HasData -eq $false}
Add-DPMDisk $dpmdisks
```

Należy pamiętać, że ten krok obejmuje skonfigurowanie puli magazynów jako dysku lub dysków, na których program DPM przechowuje repliki i punkty odzyskiwania chronionych danych. Ta pula jest częścią konfiguracji programu DPM i jest inna niż pula miejsc do magazynowania służąca do tworzenia woluminów danych opisanych w poprzedniej sekcji. Aby uzyskać więcej informacji na temat pul magazynów programu DPM, zobacz [Konfigurowanie magazynu dysków i pul magazynów](#).

Konfigurowanie klastra serwera plików systemu Windows

Deduplikacja wymaga specjalnego zestawu opcji konfiguracji, który umożliwi obsługę zwirtualizowanego magazynu programu DPM z uwzględnieniem skali danych i rozmiaru poszczególnych plików. Są to opcje globalne względem klastra lub węzła klastra. W każdym węźle klastra należy włączyć deduplikację i indywidualnie skonfigurować ustawienia klastra.

1. **Włącz deduplikację w magazynie serwera plików systemu Windows** — rolę deduplikacji należy zainstalować na wszystkich węzłach klastra serwera plików systemu Windows. W tym celu uruchom następujące polecenie programu PowerShell w każdym węźle klastra:

```
Install-WindowsFeature -Name FileAndStorage-Services,FS-Data-Deduplication -ComputerName <node name>
```

2. **Dopasuj przetwarzanie deduplikacji do plików danych kopii zapasowej** — uruchom następujące polecenie programu PowerShell, aby ustawić uruchamianie optymalizacji bez opóźnień i zrezygnować z optymalizacji częściowych zapisów w plikach. Należy pamiętać, że domyślnie wykonywanie zadań odzyskiwania pamięci jest zaplanowane co tydzień. Co cztery tygodnie zadanie to jest uruchamiane w trybie głębokiego odzyskiwania pamięci, który umożliwia przeprowadzenie dokładniejszego i bardziej czasochłonnego wyszukiwania danych do usunięcia. W przypadku obciążenia programu DPM tryb głębokiego odzyskiwania pamięci nie przynosi znaczących korzyści i skraca czas optymalizowania danych przy użyciu funkcji deduplikacji. Dlatego tryb głębokiego odzyskiwania pamięci jest wyłączany.

```
Set-ItemProperty -Path HKLM:\Cluster\Dedup -Name DeepGCInterval -Value 0xFFFFFFFF
```

3. **Dostosuj wydajność do wymagań operacji na dużą skalę** — uruchom następujący skrypt programu PowerShell w celu:

- wyłączenia dodatkowego przetwarzania i operacji we-wy po uruchomieniu trybu głębokiego odzyskiwania pamięci,
- zarezerwowania dodatkowej pamięci na potrzeby przetwarzania skrótów,
- włączenia optymalizacji w celu umożliwienia natychmiastowej defragmentacji dużych plików.

```
Set-ItemProperty -Path HKLM:\Cluster\Dedup -Name HashIndexFullKeyReservationPercent -Value 70  
Set-ItemProperty -Path HKLM:\Cluster\Dedup -Name EnablePriorityOptimization -Value 1
```

Te ustawienia służą do modyfikowania następujących elementów:

- HashIndexFullKeyReservationPercent: ta wartość służy do kontrolowania ilości pamięci zadania optymalizacji, która jest używana na potrzeby istniejących skrótów fragmentu w stosunku do nowych skrótów fragmentu. Na dużą skalę ustawienie 70% powoduje skuteczniejszą optymalizację przepływności niż domyślne ustawienie 50%.
- EnablePriorityOptimization: jeśli rozmiar plików zbliża się do 1 TB, fragmentacja pojedynczego pliku może spowodować zgromadzenie fragmentów, których łączny rozmiar wyniesie tyle co limit rozmiaru na plik. Przetwarzanie optymalizacji powoduje skonsolidowanie tych fragmentów i uniemożliwia osiągnięcie tego limitu. Dzięki ustawieniu tego klucza rejestru deduplikacja spowoduje dodanie dodatkowego procesu obsługującego bardzo pofragmentowane, deduplikowane pliki o wysokim priorytecie.

Konfigurowanie programu DPM i planowanie deduplikacji

Tworzenie kopii zapasowej i deduplikacja to procesy wymagające wielu operacji we/wy. Ich uruchomienie w tym samym czasie i wynikające z tego dodatkowe obciążenie podczas przełączania się między operacjami mogłoby być drogie i spowodować codzienne tworzenie kopii zapasowej bądź deduplikowanie mniejszej ilości danych. Zalecamy skonfigurowanie dedykowanych osobnych okien na potrzeby deduplikacji i tworzenia kopii zapasowej. Dzięki temu ruch we/wy dla każdej z tych operacji będzie efektywnie dystrybuowany podczas codziennego działania systemu. Podczas harmonogramowania zalecamy skorzystanie z następujących wskazówek:

- Podziel dni na nienakładające się okna tworzenia kopii zapasowej i deduplikacji.

- Skonfiguruj niestandardowe harmonogramy tworzenia kopii zapasowej.
- Skonfiguruj niestandardowe harmonogramy deduplikacji.
- Zaplanuj optymalizację w ramach okna codziennej deduplikacji.
- Skonfiguruj oddzielne weekendowe harmonogramy deduplikacji, aby wykorzystać czas w celu wykonania zadań odzyskiwania pamięci i czyszczenia danych.

Harmonogramy programu DPM można skonfigurować przy użyciu następującego polecenia programu PowerShell:

```
Set-DPMConsistencyCheckWindow -ProtectionGroup $mpg -StartTime $startTime -
DurationInHours $duration
Set-DPMBackupWindow -ProtectionGroup $mpg -StartTime $startTime -DurationInHours
$duration
```

W tej konfiguracji program DPM jest konfigurowany tak, aby kopia zapasowa maszyn wirtualnych była tworzona między 22:00 i 6:00. Deduplikacja jest zaplanowana na pozostałe 16 godzin dnia. Należy pamiętać, że rzeczywisty konfigurowany czas deduplikacji będzie zależeć od rozmiaru woluminu. Aby uzyskać więcej informacji, zobacz [Ustalanie rozmiaru woluminów na potrzeby deduplikacji danych](#). Okno deduplikacji o długości 16 godzin rozpoczynające się o 6:00 po zakończeniu okna tworzenia kopii zapasowej należy skonfigurować w następujący sposób w dowolnym węźle klastra:

```
#disable default schedule
Set-DedupSchedule * -Enabled:$false
#Remainder of the day after an 8 hour backup window starting at 10pm $dedupDuration = 16
$dedupStart = "6:00am"
#On weekends GC and scrubbing start one hour earlier than optimization job.
# Once GC/scrubbing jobs complete, the remaining time is used for weekend
# optimization.
$shortenedDuration = $dedupDuration - 1
$dedupShortenedStart = "7:00am"
#if the previous command disabled priority optimization schedule
#reenable it
if ((Get-DedupSchedule -name PriorityOptimization -ErrorAction SilentlyContinue) -ne $null)
{
Set-DedupSchedule -Name PriorityOptimization -Enabled:$true
}
#set weekday and weekend optimization schedules
New-DedupSchedule -Name DailyOptimization -Type Optimization -DurationHours $dedupDuration -Memory 50 -
Priority Normal -InputOutputThrottleLevel None -Start $dedupStart -Days
Monday,Tuesday,Wednesday,Thursday,Friday
New-DedupSchedule -Name WeekendOptimization -Type Optimization -DurationHours $shortenedDuration -Memory 50 -
Priority Normal -InputOutputThrottleLevel None -Start $dedupShortenedStart -Days Saturday,Sunday
#re-enable and modify scrubbing and garbage collection schedules
Set-DedupSchedule -Name WeeklyScrubbing -Enabled:$true -Memory 50 -DurationHours $dedupDuration -Priority
Normal -InputOutputThrottleLevel None -Start $dedupStart -StopWhenSystemBusy:$false -Days Sunday
Set-DedupSchedule -Name WeeklyGarbageCollection -Enabled:$true -Memory 50 -DurationHours $dedupDuration -
Priority Normal -InputOutputThrottleLevel None -Start $dedupStart -StopWhenSystemBusy:$false -Days Saturday
#disable background optimization
if ((Get-DedupSchedule -name BackgroundOptimization -ErrorAction SilentlyContinue) -ne $null)
{
Set-DedupSchedule -Name BackgroundOptimization -Enabled:$false
}
```

Podczas każdorazowego modyfikowania okna tworzenia kopii zapasowej należy pamiętać o równoczesnym zmodyfikowaniu okna deduplikacji tak, aby okna te się nie nakładały. Okna deduplikacji i tworzenia kopii zapasowej nie muszą wypełniać wszystkich 24 godzin dnia. Zdecydowanie zaleca się pozostawienie czasu na ewentualne zmiany czasu przetwarzania wynikające z oczekiwanych dziennych zmian obciążeń i fragmentów danych.

Wpływ na wydajność tworzenia kopii zapasowej

Po zakończeniu deduplikacji zestawu plików można zauważyć nieznaczny spadek wydajności podczas uzyskiwania dostępu do plików. Wynika on z dodatkowych operacji przetwarzania wymaganych do uzyskiwania dostępu do używanego formatu deduplikowanych plików. W tym scenariuszu pliki są zestawem plików VHDX z ciągłym wykorzystaniem w programie DPM podczas tworzenia kopii zapasowych. Jeśli te pliki są deduplikowane, operacje tworzenia kopii zapasowej i odzyskiwania danych mogą przebiegać wolniej niż bez deduplikacji. Podobnie jak w przypadku każdego produktu do tworzenia kopii zapasowej, program DPM stanowi obciążenie intensywnie wykorzystujące operacje zapisu, a operacje odczytu są najważniejsze podczas procesów odzyskiwania danych. Poniżej podano zalecenia dotyczące wpływu procesu deduplikacji na wydajność tworzenia kopii zapasowej.

- Operacje odczytu/przywracania: wpływ na operacje odczytu jest przeważnie nieistotny i nie wymaga uwagi użytkownika, ponieważ funkcja deduplikacji buforuje deduplikowane fragmenty.
- Operacje zapisu/tworzenia kopii zapasowej: podczas definiowania okna tworzenia kopii zapasowej należy zaplanować wzrost czasu tworzenia kopii zapasowej o około 5–10%. (Jest to wzrost porównywany z oczekiwanym czasem tworzenia kopii zapasowej podczas zapisywania na -woluminach niededuplikowanych.)

Monitorowanie

Program DPM i deduplikację danych można monitorować w celu zapewnienia, że:

- Ilość miejsca na dysku, dla której zainicjowano obsługę administracyjną, jest wystarczająca do przechowywania danych kopii zapasowej.
- Zadania tworzenia kopii zapasowej programu DPM są kończone w zwykły sposób.
- Na woluminach kopii zapasowej włączono deduplikację.
- Harmonogramy deduplikacji zostały prawidłowo ustawione.
- Przetwarzanie deduplikacji jest codziennie wykonywane w zwykły sposób.
- Wielkość oszczędności wynikających z deduplikacji odpowiada założeniom dla konfiguracji systemu.

Powodzenie deduplikacji zależy od ogólnych możliwości sprzętu systemu (w tym od szybkości przetwarzania procesora CPU, przepustowości operacji we/wy, pojemności magazynu), prawidłowej konfiguracji systemu, średniego obciążenia systemu i codziennej ilości modyfikowanych danych.

Program DPM można monitorować przy użyciu centralnej konsoli programu DPM. Zobacz [Instalowanie konsoli centralnej](#).

Deduplikację można monitorować w celu sprawdzania jej stanu, wielkości oszczędności oraz stanu harmonogramu przy użyciu następującego polecenia programu PowerShell:

Uzyskaj informacje na temat stanu:

```
PS C:\> Get-DedupStatus
FreeSpace SavedSpace OptimizedFiles InPolicyFiles Volume
-----
280.26 GB 529.94 GB 36124 36125 X:
151.26 GB 84.19 GB 43017 43017 Z:
```

Uzyskaj informacje na temat oszczędności:

```
PS C:\> Get-DedupVolume
Enabled SavedSpace SavingsRate Volume
-----
True 529.94 GB 74 % X:
```

Aby uzyskać informacje na temat stanu harmonogramu, użyj polecenia cmdlet Get-DedupSchedule.

Monitorowanie zdarzeń

Monitorowanie dziennika zdarzeń może pomóc w zrozumieniu deduplikacji zdarzeń i stanu.

- Aby przejrzeć zdarzenia deduplikacji, w **Eksploratorze plików** przejdź kolejno do pozycji **Dzienniki aplikacji i usług > Microsoft > Windows > Deduplikacja**.
- Jeśli wartość **LastOptimizationResult = 0x00000000** pojawia się w wynikach polecenia Get-DedupStatus |fl programu Windows PowerShell, cały zestaw danych został przetworzony podczas poprzedniego zadania optymalizacji. W przeciwnym razie system nie mógł ukończyć przetwarzania deduplikacji — należy sprawdzić ustawienia konfiguracji, na przykład rozmiar woluminu.

Aby zapoznać się z bardziej szczegółowymi przykładami poleceń cmdlet, zobacz [Monitorowanie deduplikacji danych i tworzenie powiązanych raportów](#).

Monitorowanie magazynu kopii zapasowych

W naszym przykładzie konfiguracji woluminy 7,2 TB są wypełniane 10 TB danych „logicznych” (rozmiar danych niededuplikowanych) przechowywanych w 10 dynamicznych plikach VHDX o rozmiarze 1 TB. Ze względu na to, że dodatkowe dane kopii zapasowej będą gromadzone w tych plikach, pojemność woluminu będzie powoli wypełniana. Jeśli wartość procentowa oszczędności wynikających z deduplikacji jest wystarczająco wysoka, wszystkie 10 plików będzie mogło osiągnąć maksymalny rozmiar logiczny i nadal mieścić się na woluminie 7,2 TB (potencjalnie może nawet istnieć dodatkowe miejsce do użycia na potrzeby przydzielania dodatkowych plików VHDX na serwerach programu DPM). Ale jeśli oszczędności rozmiaru wynikające z deduplikacji nie są wystarczające, wolumin może być pełny (może zabraknąć na nim miejsca), zanim pliki VHDX osiągną pełen rozmiar logiczny. Aby zapobiec zapełnianiu woluminów, zalecamy:

- Zastosowanie ostrożnego podejścia do wymagań dotyczących rozmiaru woluminów oraz zezwolenie na nadmiarowe inicjowanie obsługi administracyjnej magazynu. Zaleca się zapewnienie bufora o wielkości co najmniej 10% podczas planowania użycia magazynu kopii zapasowej. Bufor ten będzie przeznaczony do obsługi oczekiwanych zmian fragmentów danych i oszczędności wynikających z deduplikacji.
- Monitorowanie woluminów używanych na potrzeby magazynu kopii zapasowej w celu zapewnienia wykorzystania miejsca i wielkości oszczędności wynikających z deduplikacji na oczekiwanym poziomie.

Jeśli wolumin jest pełen, można zauważyć następujące symptomy:

- Maszyna wirtualna programu DPM będzie mieć krytyczny stan wstrzymania i nie będzie wydawać żadnych dodatkowych zadań tworzenia kopii zapasowej.
- Wszystkie zadania kopii zapasowej, które korzystają z plików VHDX na pełnym woluminie, zakończą się niepowodzeniem.

Aby przywrócić normalne działanie systemu po zaistnieniu tej sytuacji, można zainicjować obsługę administracyjną dodatkowego magazynu i przeprowadzić migrację magazynu maszyny wirtualnej programu DPM lub jej pliku VHDX w celu zwolnienia miejsca:

1. Zatrzymaj serwer programu DPM, który jest właścicielem plików VHDX w pełnym udziale kopii zapasowej.
2. Utwórz dodatkowy udział woluminu i kopii zapasowej przy użyciu konfiguracji i ustawień używanych już do istniejących udziałów, takich jak ustawienia systemu plików NTFS i deduplikacji.

3. **Przeprowadź migrację magazynu** maszyny wirtualnej serwera programu DPM oraz migrację co najmniej jednego pliku VHDX z pełnego udziału kopii zapasowej do nowego udziału kopii zapasowej utworzonego w ramach kroku 2.
4. Uruchom zadanie odzyskiwania pamięci deduplikacji danych w źródłowym udziale kopii zapasowej, który jest pełny. To zadanie odzyskiwania pamięci powinno zakończyć się pomyślnie i spowodować odzyskanie wolnego miejsca.
5. Uruchom ponownie maszynę wirtualną serwera programu DPM.
6. Po rozpoczęciu następnego okna kopii zapasowej dla wszystkich źródeł danych z błędami zostanie wyzwolone zadanie sprawdzania spójności programu DPM.
7. Wszystkie zadania tworzenia kopii zapasowej powinny teraz zakończyć się pomyślnie.

Podsumowanie

Połączenie deduplikacji z programem DPM umożliwia uzyskiwanie znacznych oszczędności miejsca. Dzięki temu można przechowywać większe ilości danych, częściej tworzyć kopie zapasowe i obniżać całkowity koszt posiadania powiązany z wdrożeniem programu DPM. Wskazówki i zalecenia przedstawione w tym dokumencie powinny udostępnić narzędzia i wiedzę umożliwiające skonfigurowanie deduplikacji dla magazynu programu DPM oraz uzyskiwanie korzyści we własnych wdrożeniach.

Często zadawane pytania

Pyt.: Pliki VHDX programu DPM muszą mieć rozmiar 1 TB. Czy oznacza to, że program DPM nie może utworzyć kopii zapasowej maszyny wirtualnej, elementu programu SharePoint, bazy danych SQL ani pliku o rozmiarze większym niż 1 TB?

Odp.: Nie. Program DPM agreguje wiele woluminów na potrzeby przechowywania kopii zapasowych. Dlatego rozmiar pliku wynoszący 1 TB nie ma żadnego wpływu na rozmiary źródeł danych, których kopie zapasowe mogą być wykonywane w programie DPM.

Pyt.: Wygląda na to, że pliki VHDX magazynu programu DPM muszą być wdrażane tylko w zdalnych udziałach plików SMB. Co się stanie, jeśli będę przechowywać pliki VHDX na woluminach z włączoną deduplikacją w tym samym systemie, w którym działa maszyna wirtualna programu DPM?

Odp.: Jak opisano powyżej, program DPM, funkcja Hyper-V i deduplikacja to operacje z intensywnym wykorzystaniem magazynu i mocy obliczeniowej. Połączenie wszystkich trzech w jednym systemie może prowadzić do powstania operacji o intensywnym wykorzystaniu danych we-wy i procesów, które mogą zablokować dostęp do funkcji Hyper-V oraz powiązanych z nią maszyn wirtualnych. Jeśli zdecydujesz się na eksperymentowanie podczas konfigurowania programu DPM na maszynie wirtualnej z woluminami magazynu kopii zapasowej na tym samym komputerze, musisz uważnie monitorować wydajność, aby upewnić się, że przepustowość operacji we-wy i moce obliczeniowe wystarczają do obsługi wszystkich operacji na jednym komputerze.

Pyt.: Zalecane jest użycie dedykowanych osobnych okien na potrzeby deduplikacji i tworzenia kopii zapasowej. Dlaczego nie mogę włączyć deduplikacji podczas tworzenia kopii zapasowej programu DPM? Muszę tworzyć kopię zapasową mojej bazy danych SQL co 15 minut.

Odp.: Deduplikacja i program DPM stanowią operacje o znacznym wykorzystaniu magazynu. Ich równoczesne uruchamianie może być mało wydajne i prowadzić do zablokowania operacji we/wy. Dlatego aby chronić obciążenia więcej niż raz dziennie (na przykład program SQL Server co 15 minut) i aby w tym samym czasie włączyć deduplikację, upewnij się, że przepustowość operacji we/wy i możliwości komputera są wystarczające do uniknięcia zablokowania zasobów.

Pyt.: W opisanej konfiguracji program DPM należy uruchomić na maszynie wirtualnej. Dlaczego nie mogę

włączyć deduplikacji bezpośrednio na woluminie repliki i woluminach kopii w tle zamiast na plikach VHDX?

Odp.: Deduplikacja jest przeprowadzana na poszczególnych woluminach działających w powiązaniu z pojedynczymi plikami. Ponieważ deduplikacja powoduje optymalizację na poziomie plików, nie może ona obsługiwać technologii VolSnap, której program DPM używa do przechowywania danych kopii zapasowej. Po uruchomieniu programu DPM na maszynie wirtualnej funkcja Hyper-V mapuje operacje woluminu programu DPM do poziomu pliku VHDX. Pozwala to funkcji deduplikacji na optymalizowanie danych kopii zapasowych i zapewnianie większych oszczędności pojemności magazynu.

Pyt.: Powyższa przykładowa konfiguracja powoduje utworzenie tylko woluminów o rozmiarze 7,2 TB. Czy mogę tworzyć woluminy większe lub mniejsze?

Odp.: Funkcja deduplikacji uruchamia jeden wątek na każdym woluminie. Wzrost rozmiaru woluminu spowoduje, że deduplikacja będzie wymagać dłuższego czasu, aby ukończyć jego optymalizację. Z drugiej strony małe woluminy oznaczają małą ilość danych, w obrębie których można znaleźć zduplikowane fragmenty, a co za tym idzie, oszczędności mogą być mniejsze. Dlatego też w celu uzyskania optymalnych oszczędności zaleca się dostosowywanie rozmiaru woluminu na podstawie łącznej wielkości fragmentów i sprzętu w systemie. Więcej szczegółowych informacji na temat określania rozmiarów woluminów używanych podczas deduplikacji można znaleźć w części [Ustalanie rozmiarów woluminów na potrzeby deduplikacji w systemie Windows Server](#). Więcej szczegółowych informacji na temat określania rozmiarów woluminów używanych podczas deduplikacji można znaleźć w części [Ustalanie rozmiarów woluminów na potrzeby deduplikacji danych](#).

Wdrażanie agenta ochrony programu DPM

11.12.2019 • 20 minutes to read

Agent ochrony programu System Center Data Protection Manager (DPM) to oprogramowanie, które można zainstalować na każdym komputerze zawierającym dane, których kopię zapasową chcesz utworzyć przy użyciu programu DPM. Agent ochrony składa się z dwóch elementów — samego agenta ochrony oraz koordynatora agenta. Oto, jakie pełni funkcje:

- Identyfikuje dane, które program DPM może chronić i odzyskiwać.
- Zezwala serwerowi programu DPM na przeglądanie udziałów, woluminów i folderów na komputerze chronionym.
- Tworzy oddzielny dziennik zmian dla każdego chronionego woluminu i przechowuje ten dziennik na woluminie w ukrytym pliku. Rejestruje w dzienniku zmiany wszystkie zmiany chronionych danych i transferuje dziennik z komputera chronionego do serwera programu DPM, aby umożliwić programowi DPM synchronizację danych podstawowych z repliką.

Skonfiguruj agenta w następujący sposób:

- Jeśli komputer zawierający dane, dla których chcesz wykonać kopię zapasową, znajduje się za zaporą, należy [skonfigurować wyjątki zapory](#).
- Jeśli komputer nie znajduje się za zaporą lub wyjątki zapory zostały już skonfigurowane w celu zezwolenia na dostęp, możesz [zainstalować agenta z konsoli programu DPM](#).
- Jeśli nie masz dostępu za pośrednictwem zapory albo komputer, który ma być chroniony, jest w grupie roboczej lub w niezaufanej domenie, albo po prostu konieczne jest użycie innej metody instalacji, możesz [zainstalować agenta ręcznie](#), a następnie [dołączyć agenta](#).

Konfigurowanie wyjątków zapory

Aby agent ochrony mógł komunikować się z serwerem programu DPM przez zaporę, wymagane jest wprowadzenie wyjątków zapory.

Skonfiguruj wyjątek ruchu przychodzącego dla programu sqsqr.exe dla wystąpienia DPM programu SQL Server, aby umożliwić ruch TCP na porcie 80. Serwer raportów nasłuchuje żądań HTTP na porcie 80. W poniższej tabeli przedstawiono protokoły i porty wymagane do komunikacji między serwerem DPM i chronionymi serwerami i klientami.

PROTOKÓŁ	PORT	SZCZEGÓŁY
----------	------	-----------

PROTOKÓŁ	PORT	SZCZEGÓŁY
DCOM	135/TCP (dynamiczny)	Protokół kontroli programu DPM używa protokołu DCOM. Program DPM wydaje polecenia agentowi ochrony za pomocą wywołania DCOM dla agenta. Agent ochrony odpowiada wywołaniem DCOM dla serwera programu DPM. Port TCP o numerze 135 to punkt rozwiązywania punktu końcowego zabezpieczeń DCE używany przez protokół DCOM. Domyślnie protokół DCOM przypisuje porty dynamicznie z zakresu portów TCP od 1024 do 65 535. Ten zakres można jednak skonfigurować przy użyciu usług składowych. Należy pamiętać, że aby umożliwić komunikację między programem DPM i agentem, należy otworzyć górny zakres portów 1024-65535. Aby otworzyć porty, należy wykonać następujące czynności: 1. w Menedżerze usług IIS 7,0 w okienku połączenia kliknij węzeł poziomu serwera w drzewie. 2. Kliknij dwukrotnie ikonę Obsługa zapory FTP na liście funkcji. 3. Wprowadź zakres wartości dla zakresu portów kanału danych. 4. po wprowadzeniu zakresu portów dla usługi FTP w okienku Akcje kliknij przycisk Zastosuj , aby zapisać ustawienia konfiguracji.
TCP	5718/TCP 5719/TCP	Kanał danych programu DPM korzysta z protokołu TCP. Zarówno program DPM, jak i chronione komputery inicjują połączenia, aby zezwolić programowi DPM na wykonywanie takich operacji, jak synchronizacja i odzyskiwanie. Program DPM komunikuje się z koordynatorem agenta przez port 5718 oraz z agentem ochrony przez port 5719.
systemem DNS,	53/UDP	Używany do rozpoznawania nazwy hosta podczas komunikacji między programem DPM a kontrolerem domeny oraz między komputerem chronionym a kontrolerem domeny.

PROTOKÓŁ	PORT	SZCZEGÓŁY
Kerberos	88/UDP 88/TCP	Używany do uwierzytelniania punktu końcowego połączenia podczas komunikacji między programem DPM a kontrolerem domeny oraz między komputerem chronionym a kontrolerem domeny.
LDAP	389/TCP 389/UDP	Używany do przesyłania zapytań podczas komunikacji między programem DPM a kontrolerem domeny.
NetBIOS	137/UDP 138/UDP 139/TCP 445/TCP	Używany do wykonywania różnych operacji podczas komunikacji między programem DPM a komputerem chronionym, między programem DPM a kontrolerem domeny oraz między komputerem chronionym a kontrolerem domeny. Używany do ruchu SMB obsługiwanego bezpośrednio przez protokół TCP/IP na potrzeby funkcji programu DPM.

Instalowanie agenta z konsoli programu DPM

1. W konsoli administratora programu DPM kliknij pozycję **Zarządzanie > Agenci**. Kliknij pozycję **Zainstaluj** na wstążce narzędzia, aby otworzyć Kreatora instalacji agenta ochrony.
2. Na stronie **Wybierz metodę wdrożenia agenta** kliknij pozycję **Zainstaluj agentów > Dalej**.
3. Na stronie **Wybierz komputery** program DPM wyświetli listę komputerów dostępnych w tej samej domenie co serwer programu DPM. Dodaj wymagany komputer.
 - Przy pierwszym użyciu kreator programu DPM odpytuje usługę Active Directory o listę dostępnych komputerów. Po pierwszej instalacji program DPM przechowuje listę komputerów ze swojej bazy danych, która jest aktualizowana raz dziennie przez proces autowykrywania.
 - Aby znaleźć w innej domenie komputer mający dwukierunkową relację zaufania z domeną, w której znajduje się serwer programu DPM, należy wpisać w pełni kwalifikowaną nazwę domeny komputera, który ma być chroniony (na przykład *<komputer1>. Domain1.contoso.com*, gdzie *Komputer1* to nazwa komputera, który ma być chroniony, a *Domain1.contoso.com* to domena, do której należy komputer docelowy.
 - Przycisk **Zaawansowane** jest aktywny tylko wtedy, gdy do instalacji na komputerach jest dostępna więcej niż jedna wersja agenta ochrony. Jeśli przycisk jest aktywny, można go użyć, aby zainstalować poprzednią wersję agenta ochrony, która została zainstalowana przed uaktualnieniem serwera programu DPM do nowszej wersji.
4. Na stronie **Wprowadzanie poświadczeń** wpisz nazwę użytkownika i hasło konta domeny, które jest członkiem lokalnej grupy administratorów na wszystkich wybranych komputerach.
 - W polu **Domena** zaakceptuj lub wpisz nazwę domeny konta użytkownika, dla którego chcesz zainstalować agenta ochrony na komputerze docelowym. To konto może należeć do domeny, w której znajduje się serwer programu DPM, lub do domeny, która ma ustanowioną dwukierunkową relację zaufania z domeną zawierającą serwer programu DPM.

- Jeśli instalujesz agenta ochrony na komputerze w domenie zaufanej, wprowadź bieżące poświadczenia użytkownika domeny. Możesz być członkiem dowolnej domeny, która ma ustanowioną dwukierunkową relację zaufania z domeną zawierającą serwer programu DPM oraz musisz być członkiem lokalnej grupy administratorów na wszystkich komputerach docelowych, na których chcesz zainstalować agenta ochrony.
 - Jeśli wybierzesz węzeł w klastrze, program DPM wykryje wszystkie dodatkowe węzły tego klastra i wyświetli stronę **Wybierz węzły klastra**.
5. Na stronie **Wybierz węzły klastra** wybierz opcję, której program DPM ma używać podczas instalowania agentów na dodatkowych węzłach w klastrze, a następnie kliknij przycisk **Dalej**.
6. Na stronie **Wybierz metodę ponownego uruchomienia** wybierz metodę ponownego uruchomienia, która ma być używana przez wybrane komputery po zainstalowaniu agenta ochrony. Komputer rozpocznie ochronę danych dopiero po ponownym uruchomieniu. Ponowne uruchomienie jest niezbędne, aby załadować filtr woluminu używany przez program DPM do śledzenia i transferowania zmian na poziomie bloku między serwerem programu DPM a komputerami chronionymi.
- Jeśli wybrano opcję późniejszego ponownego uruchomienia komputera, stan instalacji agenta ochrony nie jest automatycznie odświeżany na karcie **Agenci** w obszarze zadań **Zarządzanie** po ponownym uruchomieniu komputera. Konieczne jest kliknięcie przycisku **Odśwież informacje**.
 - Należy pamiętać, że nie jest wymagane ponowne uruchomienie komputera, jeśli agent ochrony jest instalowany na innym serwerze DPM.
 - Jeśli jakikolwiek z wybranych komputerów jest węzłem w klastrze, zostanie wyświetlona dodatkowa strona **Wybierz metodę ponownego uruchomienia**, na której można wybrać metodę ponownego uruchomienia klastrowanych komputerów. Aby pomyślnie chronić klastrowane dane, agent ochrony musi być zainstalowany we wszystkich węzłach klastra. Komputery rozpoczną ochronę danych dopiero po ponownym uruchomieniu. Ponieważ uruchamianie usług chwilę trwa, program DPM może nawiązać kontakt z agentem w klastrze dopiero po kilku minutach od ponownego uruchomienia.
 - Program DPM nie uruchamia automatycznie ponownie komputera, który należy do klastra serwera klastrów firmy Microsoft (MSCS). Komputery w klastrze MSCS muszą zostać uruchomione ponownie ręcznie.
7. Na stronie **Podsumowanie** kliknij przycisk **Zainstaluj**, aby rozpocząć instalację. Jeśli zostanie wyświetlona Umowa licencyjna użytkownika końcowego, zaakceptuj ją, aby rozpocząć instalację. Na karcie **Zadanie** strony instalacji możesz sprawdzić, czy instalacja powiodła się. Opcję **Zamknij** można kliknąć przed zakończeniem pracy kreatora, a następnie monitorować postępy instalacji na karcie **Agenci** w obszarze zadań **Zarządzanie**. Jeśli instalacja się nie powiedzie, alerty możesz sprawdzić na karcie **Alerty** w obszarze zadań **Monitorowanie**.

Uwaga: Po zainstalowaniu agenta ochrony na komputerach będących częścią farmy programu Windows SharePoint Services jako komputery chronione na karcie **Agenci** w obszarze zadań **Zarządzanie** będą widoczne tylko wybrane komputery, a nie wszystkie komputery z farmy. Jeśli jednak farma programu Windows SharePoint Services zawiera dane na wybranych komputerach, program DPM będzie chronić te dane na wszystkich komputerach w farmie, pod warunkiem że na wszystkich z nich jest zainstalowany agent ochrony.

Zainstaluj agenta ręcznie

1. Jeśli zainstalujesz agenta na komputerze za zaporą, musisz sprawdzić, czy agenta można wypchnąć przez zaporę.

Na przykład możesz uruchomić następujące polecenie na komputerze, aby skonfigurować Zaporę

systemu Windows: **netsh advfirewall firewall add rule name="Zezwalaj na wypchnięcie zdalnego agenta programu DPM" dir=in action=allow service=any enable=yes profile=any remoteip=<adres_IP>** , gdzie adres_IP jest adresem serwera DPM.

Aby skonfigurować wyjątek dla portu na zaporze, zobacz temat [Konfigurowanie wyjątków zapory dla agenta](#).

2. Na komputerze, który ma być chroniony, otwórz okno wiersza polecenia z podwyższonym poziomem uprawnień, a następnie uruchom następujące polecenia:

Aby przypisać literę dysku, wpisz: **net use z: \<dpmServerName>\c \$** , gdzie Z to litera dysku lokalnego, która ma zostać przypisana, a <dpmServerName> jest nazwą serwera DPM, który będzie chronić komputer.

Aby zmienić katalog, wykonaj następujące czynności:

- Dla komputera 64-bitowego wpisz **CD/d <przypisana litera dysku>: \program files\microsoft DPM\DPM\ProtectionAgents\RA\5.0. <numer kompilacji> 0 \ amd64** , gdzie <przypisane litery dysku> to litera dysku przypisana w poprzednim kroku, a <numer kompilacji> to numer najnowszej kompilacji programu DPM. Na przykład: **cd /d X:\Program Files\Microsoft DPM\DPM\ProtectionAgents\RA\3.0.7696.0\amd64**
 - W przypadku komputera 32-bitowego wpisz: **CD/d <przypisana litera dysku> : \program files\microsoft DPM\DPM\ProtectionAgents\RA\5.0. <numer kompilacji> 0 \ i386** , gdzie <przypisana litera dysku> to dysk zamapowany w poprzednim kroku, a <numer kompilacji> jest najnowszym numerem kompilacji programu DPM.
3. Aby zainstalować agenta ochrony, otwórz okno wiersza polecenia z podwyższonym poziomem uprawnień, a następnie uruchom następujące polecenia:
- W przypadku komputera 64-bitowego wpisz: **DpmAgentInstaller_x64.exe <dpmServerName>** gdzie <dpmServerName> to w pełni kwalifikowana nazwa domeny (FQDN) serwera programu DPM. Na przykład: **DPMAgentInstaller_x64.exe DPMserver1.contoso.com**
 - W przypadku komputera 32-bitowego wpisz: **DpmAgentInstaller_x86.exe** gdzie <dpmServerName> to w pełni kwalifikowana nazwa domeny serwera programu DPM.

Uwaga:

- Aby przeprowadzić instalację dyskretną, można użyć opcji **/q** po poleceniu **DpmAgentInstaller_x64.exe** . Na przykład: **DpmAgentInstaller_x64.exe/q <dpmServerName>**
- Aby zaakceptować umowę licencyjną ręcznie podczas instalacji dyskretniej, użyj polecenia **DpmAgentInstaller_x64.exe /q <nazwa_serwera_DPM> /IAcceptEULA**
- W przypadku określenia w wierszu polecenia nazwy serwera programu DPM nastąpi instalacja agenta ochrony oraz automatyczne skonfigurowanie kont zabezpieczeń, uprawnień oraz wyjątków zapory umożliwiających komunikację agenta ze wskazanym serwerem programu DPM. Jeśli nie określono nazwy serwera, otwórz wiersz polecenia z podwyższonym poziomem uprawnień na komputerze docelowym i wykonaj następujące czynności:
 - a. Aby zmienić typ katalogu: **CD/d <dysk systemowy> : \Program Files\Microsoft Data Protection Manager\DPM\bin**
 - b. Wpisz: **SetDpmServer.exe-dpmServerName <dpmServerName>** . Powoduje to skonfigurowanie zabezpieczeń kont, uprawnień i wyjątków zapory dla agenta w celu

umożliwienia komunikacji z serwerem.

4. Jeśli komputer docelowy został dodany do serwera programu DPM przed zainstalowaniem agenta, serwer programu DPM rozpocznie tworzenie kopii zapasowych danych komputera chronionego. Jeśli agent został zainstalowany przed dodaniem komputera do serwera programu DPM, komputer należy dołączyć, zanim serwer programu DPM rozpocznie tworzenie kopii zapasowych.

Dołącz agenta

W niektórych przypadkach po ręcznym zainstalowaniu agentów programu DPM konieczne jest dołączenie agenta do serwera DPM.

1. W konsoli administratora programu DPM na pasku nawigacyjnym kliknij pozycję **Zarządzanie > Agenci**. W okienku **Akcje** kliknij pozycję **Zainstaluj**.
2. Na stronie **Wybierz metodę wdrożenia agenta** wybierz pozycję **Dołącz agentów > Komputer w zaufanej domenie > Dalej**. Zostanie otwarty Kreator instalacji agenta ochrony.
3. Na stronie Wybierz komputery program DPM wyświetli listę komputerów dostępnych w tej samej domenie, w której znajduje się serwer DPM. Wybierz co najmniej jeden komputer (maksymalnie 50) z listy **Nazwa komputera**, a następnie wybierz pozycję **Dodaj > Dalej**.
 - Jeśli kreator jest używany po raz pierwszy, program DPM wysyła do usługi Active Directory zapytanie w celu pobrania listy potencjalnych komputerów. Po pierwszej instalacji program DPM wyświetla listę komputerów ze swojej bazy danych, która jest aktualizowana raz dziennie przez proces autowykrywania.
 - Aby dodać wiele komputerów za pomocą pliku tekstowego, kliknij przycisk **Dodaj z pliku**, a następnie w oknie dialogowym **Dodaj z pliku** wpisz lokalizację pliku tekstowego lub kliknij przycisk Przeglądaj, aby przejść do jego lokalizacji.
4. Na stronie Wprowadź poświadczenia wpisz nazwę użytkownika i hasło konta domeny, które należy do lokalnej grupy Administratorzy na wszystkich wybranych komputerach. W polu **Domena** zaakceptuj lub wpisz nazwę domeny konta użytkownika, dla którego chcesz zainstalować agenta ochrony na komputerze docelowym. To konto może należeć do domeny, w której znajduje się serwer DPM, lub do domeny zaufanej. Jeśli instalujesz agenta ochrony na komputerze w domenie zaufanej, wprowadź bieżące poświadczenia użytkownika domeny. Możesz być członkiem dowolnej zaufanej domeny oraz musisz być członkiem lokalnej grupy administratorów na wszystkich komputerach docelowych, które chcesz chronić.
5. Na stronie Podsumowanie kliknij pozycję **Dołącz**.

Wdrażanie grup ochrony

10.01.2020 • 21 minutes to read

Grupa ochrony programu System Center Data Protection Manager (DPM) to kolekcja źródeł danych, takich jak woluminy, udziały lub obciążenia aplikacji, które mają wspólne ustawienia tworzenia kopii zapasowych i przywracania. Ustawienia grupy ochrony określają:

- **Źródła danych** — serwery, komputery i obciążenia, które mają być chronione.
- **Magazyn kopii zapasowych** — sposób krótko- i długoterminowego przechowywania kopii zapasowych chronionych danych.
- **Punkty odzyskiwania** — punkty odzyskiwania, z których można odzyskać replikowane dane.
- **Przydzielono miejsce na dysku** — miejsce na dysku przydzielono do danych z puli magazynów.
- **Replikacja początkowa** — sposób obsługi początkowej replikacji danych: za pośrednictwem sieci lub ręcznie offline.
- **Sprawdzanie spójności** — sposób sprawdzania spójności replikowanych danych.

W tematach tej sekcji zamieszczono wytyczne ułatwiające podjęcie decyzji dotyczących tworzenia grupy ochrony.

Planowanie grup ochrony

Należy podjąć decyzję:

- Jak grupować zasoby, dla których chcesz utworzyć kopię zapasową w grupach ochrony.
- Jak przechowywać dane kopii zapasowej grupy ochrony?
- Ile miejsca do magazynowania jest wymagane do przechowywania danych dla grupy ochrony?
- Jak odzyskać dane kopii zapasowej dla grupy ochrony?

Istnieje kilka typowych sposobów organizowania grup ochrony:

- **Według komputera** — wszystkie źródła danych komputera należą do tej samej grupy ochrony. Organizacja według komputera zapewnia pojedynczy punkt korekty dla obciążeń wydajności komputera. Jednak wszystkie źródła danych mają te same ustawienia kopii zapasowej i odzyskiwania.
- **Według obciążenia** — poszczególne pliki i typy danych aplikacji są oddzielane do różnych grup ochrony. Organizowanie według obciążeń pozwala zarządzać obciążeniami jako grupą. Jednak odzyskanie serwera z wieloma aplikacjami może wymagać wielu taśm z różnych grup ochrony.
- **Według celu RPO/RTO** — Zbieraj źródła danych z podobnymi celami punktów odzyskiwania (RPO) i celami odzyskiwania (RTO) w grupach ochrony. Aby kontrolować cel punktu odzyskiwania, należy ustawić częstotliwość synchronizacji dla grupy ochrony, która określa ilość potencjalnej utraty danych (w czasie) podczas nieoczekiwanej awarii. RTO to akceptowalna ilość czasu, przez który dane są niedostępne. Metody magazynu wybrane dla grupy ochrony mają bezpośredni wpływ na RTO.
- **Według cech danych** — na przykład częstotliwość zmian danych, szybkość ich przyrostu lub ich wymagania dotyczące pamięci masowej.

Wybieranie nazwy grupy ochrony

Po wybraniu nazwy grupy ochrony nazwa powinna mieć znaczenie. Nazwa musi być unikatowa dla serwera programu DPM. Nazwa grupy ochrony może zawierać dowolną kombinację znaków alfanumerycznych i spacji, ale nie może być dłuższa niż 64 znaków. Program DPM nie obsługuje znaków specjalnych, takich jak `[`, `/`, `(`, `)` lub `.`.

Ustalanie ilości potrzebnego miejsca

W przypadku utworzenia grupy ochrony i wybrania ochrony opartej na dyskach konieczne jest przydzielenie miejsca w puli magazynów na repliki i punkty odzyskiwania dla wszystkich źródeł danych, dla których określono członkostwo w grupie, oraz przydzielenie miejsca na dziennik zmian na chronionych serwerach plików lub stacjach roboczych.

Aby ułatwić ustalenie pojemności miejsca do magazynowania, użyj [kalkulatora magazynu dla programu DPM z nowoczesny magazyn kopii zapasowych](#)

Program DPM zapewnia domyślne alokacje miejsca dla członków grupy ochrony. W poniższej tabeli przedstawiono, w jaki sposób program DPM oblicza alokacje domyślne.

SKŁADNIK	ALOKACJA DOMYŚLNA	LOKALIZACJA
Magazyn programu DPM	Rozmiar źródła danych x (1 + zmiana w dzienniku x zakres przechowywania w dniach x liczba kopii zapasowych dziennie) x (1,05) <i>Dla danych programu SQL Server :</i> — Rozmiar źródła danych x (1 + zmiana w dzienniku x zakres przechowywania w dniach x liczba kopii zapasowych dziennie) x (1,05) + dzienniki transakcji	Pula magazynów programu DPM lub wolumin niestandardowy
Baza danych programu DPM	2 GB (może się zwiększyć dla kopii zapasowych programu SharePoint)	Magazyn serwera DPM
Dziennik zmian (tylko do ochrony plików)	300 MB	Wolumin chroniony na serwerze plików lub stacji roboczej

- **Zmiana w dzienniku** — stawka zmian w danej bazie danych lub grupie magazynów. Zmiana w dzienniku jest różna, ale na potrzeby domyślnego zalecenia w programie DPM, zmiana w dzienniku jest definiowana jako 3%.
- **Zakres przechowywania** — określa liczbę przechowywanych punktów odzyskiwania. Domyślne zalecenie w programie DPM to pięć punktów odzyskiwania.

Po utworzeniu grupy ochrony w kolumnie **Rozmiar danych** w oknie dialogowym **Modyfikowanie przydziału dysku** wyświetlany jest link **Oblicz**. W celu wykonania początkowej alokacji dysku program DPM stosuje formuły domyślne do rozmiaru woluminu, na którym znajduje się źródło danych. Kliknij link **Oblicz**, aby zastosować formułę do rzeczywistego rozmiaru wybranego źródła danych. Program DPM określi rozmiar źródła danych i ponownie obliczy alokację dysku dla woluminów replik i punktów odzyskiwania tego źródła danych. Wykonanie tej operacji może potrwać kilka minut.

Zaakceptuj domyślne alokacje miejsca, chyba że masz pewność, że nie spełniają one Twoich potrzeb. Zastąpienie alokacji domyślnych może spowodować przydzielenie zbyt małej lub zbyt dużej ilości miejsca.

Przydzielenie punktom odzyskiwania zbyt małej ilości miejsca może uniemożliwić programowi DPM przechowywanie wystarczającej liczby punktów odzyskiwania wymaganej do spełnienia celów dotyczących

zakresu przechowywania. Przydzielenie zbyt dużej ilości miejsca marnuje miejsce na dysku.

Po utworzeniu grupy ochrony, jeśli przydzielono zbyt mało miejsca dla źródła danych, zwiększ alokację dla woluminów repliki i punktu odzyskiwania dla każdego źródła danych.

W przypadku przydzielenia zbyt dużej ilości miejsca dla grupy ochrony Usuń źródło danych z grupy ochrony i Usuń replikę, a następnie Dodaj źródło danych do grupy ochrony z mniejszymi alokacjami.

Konfigurowanie grup ochrony

Podczas konfigurowania grupy ochrony konieczne będzie wykonanie następujących czynności:

Przed rozpoczęciem

Uwagi dotyczące tworzenia grup ochrony:

- Jeśli kopie zapasowe są zapisywane na taśmie i dostępna jest tylko jedna autonomiczna stacja taśm, należy użyć pojedynczej grupy ochrony, aby zminimalizować konieczność zmieniania taśm. Wiele grup ochrony wymaga oddzielnej taśmy do każdej grupy ochrony.
 - Źródła danych na komputerze muszą być chronione przez ten sam serwer programu DPM. W programie DPM źródło danych jest woluminem, udziałem, bazą danych lub grupą magazynów, które są członkiem danej grupy ochrony.
 - Grupa ochrony może zawierać źródła danych z wielu komputerów.
 - Członków grupy ochrony nie można przenosić między grupami ochrony. Jeśli użytkownik zdecyduje później, że dany członek grupy ochrony musi być w innej grupie ochrony, należy go usunąć z danej grupy ochrony, a następnie dodać do innej grupy ochrony.
 - Jeśli członkowie grupy ochrony nie wymagają już ochrony, Zatrzymaj ochronę grupy ochrony. Po zatrzymaniu ochrony użytkownik może zachować lub usunąć chronione dane.
 - **Opcja Zachowaj chronione dane:** zachowuje replikę na dysku wraz ze skojarzonymi punktami odzyskiwania i taśmami dla określonego zakresu przechowywania.
 - **Opcja Usuń chronione dane:** usuwa replikę z dysku i wygasza dane na taśmach.
 - Po zaznaczeniu udziału lub folderu nadrzędnego jego podfoldery zostaną zaznaczone automatycznie. Można wyznaczać podfoldery do wykluczenia oraz wykluczać typy plików według rozszerzeń.
 - Należy sprawdzić, czy pojedynczy wolumin nie zawiera więcej niż 100 źródeł danych podlegających ochronie. Jeśli tak, należy w miarę możliwości rozpowszechnić źródła danych na wielu woluminach.
 - Po wybraniu źródła danych zawierającego punkt ponownej analizy program DPM pyta, czy dołączać miejsce docelowe punktu ponownej analizy do grupy ochrony. Punkty instalacji i punkty połączenia to źródła danych zawierające punkty ponownej analizy. W przypadku uwzględnienia punktu ponownej analizy nie jest replikowany; podczas odzyskiwania danych należy ręcznie utworzyć ponownie punkt ponownej analizy.
- Grupy ochrony są tworzone przy użyciu Kreatora tworzenia nowej grupy ochrony z następującymi ustawieniami:
- **Wybierz członków grupy:** określ komputery i źródła, dla których chcesz wykonywać kopie zapasowe.
 - **Wybierz metodę ochrony danych:** określ, jak chcesz obsługiwać krótkoterminowe i długoterminowe kopie zapasowe. Krótkoterminowa kopia zapasowa jest zawsze najpierw tworzona na dysku z opcją przeniesienia kopii zapasowej z dysku do chmury platformy Azure za pomocą usługi Azure Backup (na potrzeby przechowywania krótkoterminowego lub długoterminowego). Zamiast długoterminowej kopii zapasowej w chmurze możesz również skonfigurować długoterminową kopię zapasową na autonomicznym urządzeniu taśmowym lub w bibliotece taśm połączonej z serwerem programu DPM.

- **Wybierz cele krótkoterminowe:** określ sposób tworzenia kopii zapasowej w krótkoterminowym magazynie na dysku. W obszarze **Zakres przechowywania** określ, jak długo chcesz przechowywać dane na dysku. W obszarze Częstotliwość synchronizacji określ, jak często chcesz zapisywać przyrostowe kopie zapasowe na dysku. Jeśli nie chcesz ustawiać interwału kopii zapasowych, możesz zaznaczyć opcję **Zaraz** przed punktem odzyskiwania, aby program DPM wykonywał ekspresową pełną kopię zapasową bezpośrednio przed każdym zaplanowanym punktem odzyskiwania.
- **Określ cele długoterminowe:** określ, jak długo chcesz przechowywać dane na taśmie (1–99 lat). W obszarze Częstotliwość wykonywania kopii zapasowych określ, jak często mają być wykonywane kopie zapasowe na taśmie. Częstotliwość zależy od wybranego zakresu przechowywania:
 - Gdy zakres przechowywania wynosi 1–99 lat, można wybrać tworzenie kopii zapasowej codziennie, co tydzień, co dwa tygodnie, co miesiąc, co kwartał, co pół roku lub co rok.
 - Gdy zakres przechowywania wynosi 1–11 miesięcy, można wybrać tworzenie kopii zapasowej codziennie, co tydzień, co dwa tygodnie lub co miesiąc.
 - Gdy zakres przechowywania wynosi 1–4 tygodnie, można wybrać tworzenie kopii zapasowej codziennie lub co tydzień.

Należy także określić urządzenie taśmowe/bibliotekę, która ma być używana, oraz czy dane mają być kompresowane i szyfrowane na taśmie.

- **Przejrzyj przydział dysku:** przejrzyj miejsce w puli magazynu przydzielone danej grupie ochrony. Program DPM zapewnia zalecany rozmiar. Możesz zaznaczyć opcję **Automatycznie rozszerzaj woluminy**, aby automatycznie zwiększać rozmiar, gdy potrzeba więcej miejsca na dysku dla kopii zapasowej.
- **Wybierz metodę tworzenia repliki:** określ, jak chcesz obsługiwać pełną replikację początkową danych. W przypadku wybrania replikowania za pośrednictwem sieci zaleca się wybranie czasu w godzinach małego obciążenia sieci. W przypadku dużych ilości danych lub nieoptymalnych warunków sieciowych należy wziąć pod uwagę replikację danych w trybie offline za pomocą nośników wymiennych.
- W obszarze **Wybierz opcje sprawdzania spójności** wybierz sposób automatyzacji sprawdzania spójności. Można włączyć uruchamianie sprawdzania tylko wtedy, gdy dane są niespójne, lub zgodnie z harmonogramem. Jeśli nie chcesz konfigurować automatycznego sprawdzania spójności, w dowolnym momencie możesz uruchomić sprawdzanie ręczne.
- **Określ dane chronione w trybie online:** jeśli chcesz wykonywać kopie zapasowe w chmurze za pomocą usługi Azure Backup, określ ilości danych, dla których chcesz wykonywać kopie zapasowe.
- **Określ harmonogram wykonywania kopii zapasowych online:** jeśli wykonujesz kopie zapasowe na platformie Azure, określ, jak często mają być wykonywane przyrostowe kopie zapasowe na platformie Azure. Wykonywanie kopii zapasowych można zaplanować na każdy dzień/tydzień/miesiąc/rok, natomiast godziny/daty pozwalają ustalić konkretny czas uruchomienia wykonywania kopii zapasowych. Kopie zapasowe mogą być tworzone maksymalnie dwa razy dziennie. Zawsze podczas wykonywania kopii zapasowej na platformie Azure jest tworzony punkt odzyskiwania danych na podstawie kopii danych przechowywanych w kopii zapasowej na dysku programu DPM.
- **Określ zasady przechowywania danych online:** jeśli wykonujesz kopie zapasowe na platformie Azure, możesz określić, jak punkty odzyskiwania tworzone na podstawie kopii zapasowych wykonywanych co dzień/tydzień/miesiąc/rok są przechowywane na platformie Azure.
- **Wybierz replikację online:** jeśli wykonujesz kopie zapasowe na platformie Azure, określ, jak dokonywana będzie pełna replikacja początkowa danych. Możesz wykonywać replikację za pośrednictwem sieci lub tworzyć kopie zapasowe offline (rozieszczanie offline). W przypadku kopii zapasowych offline używana jest funkcja Azure Import. [Przeczytaj więcej.](#)

Opcje replikacji początkowej

Podczas tworzenia grupy ochrony należy wybrać metodę tworzenia repliki początkowej, która kopiuje wszystkie wybrane do ochrony dane na serwer programu DPM, a następnie uruchamia synchronizację ze sprawdzeniem spójności dla każdej repliki.

Replikacja początkowa przez sieć

Program DPM może utworzyć repliki automatycznie przez sieć; można je również utworzyć ręcznie, przywracając dane z nośników wymiennych, na przykład z taśmy. Automatyczne tworzenie replik jest prostsze, w zależności od rozmiaru chronionych danych i prędkości sieci ręczne tworzenie replik może być jednak szybsze.

Poniższa tabela zawiera szacunkowe czasy automatycznego tworzenia replik w sieci przez program DPM na podstawie różnych rozmiarów chronionych danych i prędkości sieci, co ułatwia wybór odpowiedniej metody tworzenia replik. Założono przy tym, że sieć działa z pełną prędkością, a inne obciążenia nie rywalizują o przepustowość. Czasy są podane w godzinach.

Liczba godzin wymagana do ukończenia automatycznego tworzenia replik przy różnych prędkościach sieci

ROZMIAR CHRONIONYCH DANYCH	512 KB/S	2 MB/S	8 MB/S	32 MB/S	100 MB/S
1 GB	6	1,5	< 1	< 1	< 1
50 GB	284	71	18	5	1,5
200 GB	1137	284	71	18	6
500 GB	2844	711	178	45	15

Replikacja offline usługi Azure Backup

Gdy wykonujesz na platformie Azure kopie zapasowe danych z serwera programu DPM, możesz dokonać replikacji początkowej za pośrednictwem sieci lub przy użyciu rozmieszczania offline. [Przeczytaj więcej.](#)

Ręczna replikacja początkowa

Jeśli użytkownik wdraża program DPM w celu chronienia danych za pośrednictwem sieci WAN, a grupa ochrony zawiera więcej niż 5 GB danych, zaleca się wybór ręcznej metody tworzenia replik.

Po wybraniu ręcznego tworzenia replik program DPM określa dokładne lokalizacje na serwerze programu DPM, w których należy utworzyć repliki. Repliki są zwykle tworzone przez przywrócenie najnowszej kopii zapasowej źródła danych z nośników wymiennych, jak taśmy. Po przywróceniu danych można ukończyć proces, uruchamiając synchronizację ze sprawdzaniem spójności wszystkich replik.

Przy przywracaniu danych na serwer programu DPM w celu utworzenia repliki należy bezwzględnie pamiętać o zachowaniu pierwotnej struktury i właściwości katalogów źródła danych, w tym sygnatur czasowych i uprawnień zabezpieczeń. Im więcej rozbieżności między replikami i chronionym źródłem danych, tym dłużej zajmuje sprawdzanie spójności w ramach całego procesu. Jeśli użytkownik nie zachowa pierwotnej struktury i właściwości katalogów, ręczne tworzenie replik może trwać tyle samo co automatyczne tworzenie replik.

Nazywanie grupy ochrony

Po nadaniu nazwy grupie ochrony Podaj unikatową, zrozumiałą nazwę grupy. Nazwa może zawierać dowolną kombinację znaków alfanumerycznych i może zawierać spacje, ale nie może przekraczać 64 znaków.

Konfigurowanie ustawień zapory w programie DPM

11.12.2019 • 10 minutes to read

Często zadawane pytania dotyczące wdrażania serwera programu System Center Data Protection Manager (DPM) oraz wdrażania agenta programu DPM mają wpływ na to, które porty muszą być otwarte na zaporze. W tym artykule omówiono porty i protokoły zapory używane przez program DPM na potrzeby ruchu sieciowego. Aby uzyskać więcej informacji dotyczących wyjątków zapory dla klientów programu DPM, przejdź do: [Configure firewall exceptions for the agent](#).

PROTOKÓŁ	PORT	SZCZEGÓŁY
DCOM	135/TCP (dynamiczny)	Protokół DCOM jest używany przez serwer programu DPM i agenta ochrony DPM do tworzenia poleceń i odpowiedzi. Program DPM wydaje polecenia agentowi ochrony za pomocą wywołania DCOM dla agenta. Agent ochrony odpowiada wywołaniem DCOM dla serwera programu DPM. Port TCP o numerze 135 to punkt rozwiązywania punktu końcowego DCE używany przez protokół DCOM. Domyślnie protokół DCOM przypisuje porty dynamicznie z zakresu portów TCP od 1024 do 65 535. Można jednak użyć usług składowych, aby dostosować zakres portów TCP. W tym celu wykonaj następujące czynności: 1. w Menedżerze usług IIS 7,0 w okienku połączenia kliknij węzeł poziomu serwera w drzewie. 2. na liście funkcji kliknij dwukrotnie ikonę Obsługa zapory FTP. 3. Wprowadź zakres wartości dla zakresu portów kanału danych dla usługi FTP. 4. w okienku Akcje kliknij pozycję Zastosuj, aby zapisać ustawienia konfiguracji.
TCP	5718/TCP 5719/TCP	Kanał danych programu DPM korzysta z protokołu TCP. Zarówno program DPM, jak i chronione komputery inicjują połączenia, aby zezwolić programowi DPM na wykonywanie takich operacji, jak synchronizacja i odzyskiwanie. Program DPM komunikuje się z koordynatorem agenta przez port 5718 oraz z agentem ochrony przez port 5719.

PROTOKÓŁ	PORT	SZCZEGÓŁY
TCP	6075/TCP	Włączony podczas tworzenia grupy ochrony, aby ułatwić ochronę komputerów klienckich. Wymagany do odzyskiwania przez użytkownika końcowego. Wyjątek Zapory systemu Windows (DPMAM_WCF_Service) dla programu Amscvhost.exe zostanie utworzony po włączeniu programu Central Console dla programu DPM w programie Operations Manager.
systemem DNS,	53/UDP	Używany do rozpoznawania nazw hostów na potrzeby komunikacji między programem DPM a kontrolerem domeny oraz między komputerem chronionym a kontrolerem domeny.
Kerberos	88/UDP 88/TCP	Używany do uwierzytelniania punktu końcowego połączenia podczas komunikacji między programem DPM a kontrolerem domeny oraz między komputerem chronionym a kontrolerem domeny.
LDAP	389/TCP 389/UDP	Używany do przesyłania zapytań podczas komunikacji między programem DPM a kontrolerem domeny.
NetBIOS	137/UDP 138/UDP 139/TCP 445/TCP	Używany do wykonywania różnych operacji podczas komunikacji między programem DPM a komputerem chronionym, między programem DPM a kontrolerem domeny oraz między komputerem chronionym a kontrolerem domeny. Używany na potrzeby funkcji programu DPM używających bloku komunikatów serwera (SMB), gdy jest on bezpośrednio hostowany przez protokół TCP/IP.

Ustawienia zapory systemu Windows

Jeśli Zapora systemu Windows jest włączona podczas instalowania programu DPM, Instalator programu DPM skonfiguruje odpowiednio ustawienia zapory systemu Windows wraz z regułami i wyjątkami. Ustawienia są podsumowane w poniższej tabeli.

Uwaga:

- Aby uzyskać informacje dotyczące konfigurowania wyjątków zapory dla komputerów chronionych za pomocą programu DPM, zobacz [Configure firewall exceptions for the agent](#).
- Jeśli Zapora systemu Windows nie była dostępna podczas instalowania programu DPM, zobacz [Ręczne konfigurowanie Zapory systemu Windows](#).

- Jeśli używasz bazy danych programu DPM na zdalnym wystąpieniu programu SQL Server, musisz skonfigurować kilka wyjątków zapory na zdalnym wystąpieniu programu SQL Server. Zapoznaj się z tematem [Konfigurowanie Zapory systemu Windows w zdalnym wystąpieniu programu SQL Server](#).

NAZWA ZASADY	SZCZEGÓŁY	PROTOKÓŁ	PORT
Ustawienie protokołu DCOM programu Microsoft System Center 2012 Data Protection Manager	Wymagane na potrzeby komunikacji DCOM między serwerem programu DPM a chronionymi komputerami.	DCOM	135/TCP (dynamiczny)
Microsoft System Center 2012 Data Protection Manager	Wyjątek dla programu Msdpmp.exe (usługi programu DPM). Uruchamiany na serwerze DPM.	Wszystkie protokoły	Wszystkie porty
Agent replikacji programu Microsoft System Center 2012 Data Protection Manager	Wyjątek dla programu Dpmra.exe (usługi agenta ochrony używanej do tworzenia kopii zapasowej i przywracania danych). Uruchamiany na serwerze DPM i komputerach chronionych.	Wszystkie protokoły	Wszystkie porty

Ręczne konfigurowanie Zapory systemu Windows

1. W Menedżerze serwera wybierz kolejno opcje **Serwer lokalny** > **Narzędzia** > **Zapora systemu Windows z zabezpieczeniami zaawansowanymi**.
2. W konsoli **zapory systemu Windows z zabezpieczeniami zaawansowanymi** Sprawdź, czy Zapora systemu Windows jest włączona dla wszystkich profili, a następnie kliknij pozycję **reguły ruchu przychodzącego**.
3. W celu utworzenia wyjątku w okienku **Akcje** kliknij pozycję **Nowa reguła**, aby otworzyć kreatora **Nowa reguła przychodząca**.

Na stronie **Typ reguły** sprawdź, czy jest wybrana opcja **Program**, a następnie kliknij przycisk **Dalej**.

4. Skonfiguruj wyjątki zgodne z domyślnymi regułami, które zostałyby utworzone przez Instalatora programu DPM, gdyby Zapora systemu Windows była włączona podczas instalowania programu DPM.
 - a. Aby ręcznie utworzyć wyjątek odpowiadający domyślnej regule Data Protection Manager programu Microsoft System Center 2012 R2 na stronie **program**, kliknij przycisk **Przeglądaj** dla pola **ścieżka tego programu**, a następnie przejdź do < **literę dysku systemowego**>: \program files\microsoft DPM\DPM\bin > **MSDPM. exe** > **Otwórz** > **dalej**.

Na stronie Akcja Pozostaw domyślne ustawienie opcji Zezwalaj na **połączenie** lub Zmień ustawienia zgodnie z wytycznymi organizacji > **dalej**.

Na stronie **profil** Pozostaw domyślne ustawienia **domeny**, **prywatnei publicznej** lub Zmień ustawienia zgodnie z wytycznymi organizacji > **dalej**.

Na stronie **Nazwa** wpisz nazwę reguły i opcjonalnie opis > **Zakończ**.

- b. Wykonaj te same kroki, aby ręcznie utworzyć wyjątek odpowiadający domyślnej regule agenta replikacji danych programu Microsoft System Center 2012 R2, przechodząc do < **literę dysku systemowego**>: \Program Files\Microsoft DPM\DPM\bin i wybierając polecenie **DPMRA. exe**.

Zwróć uwagę na to, że jeśli uruchamiasz program System Center 2012 R2 z dodatkiem SP1, domyślne reguły będą miały nazwy nadane przez program **Microsoft System Center 2012 Service Pack 1 Data Protection Manager**.

Skonfiguruj zaporę systemu Windows na zdalnym wystąpieniu SQL Server

- W przypadku używania zdalnego wystąpienia programu SQL Server jako bazy danych programu DPM musisz skonfigurować Zaporę systemu Windows na tym zdalnym wystąpieniu programu SQL Server.
- Po zakończeniu instalacji programu SQL Server protokół TCP/IP powinien być włączony dla wystąpienia programu DPM programu SQL Server z następującymi ustawieniami:
 - Domyślna inspekcja niepowodzeń
 - Włączone sprawdzanie zasad haseł
- Skonfiguruj wyjątek ruchu przychodzącego dla programu sqservr.exe dotyczący wystąpienia programu DPM programu SQL Server, aby umożliwić ruch TCP na porcie 80. Serwer raportów nasłuchuje żądań HTTP na porcie 80.
- Domyślne wystąpienie aparatu bazy danych nasłuchuje na porcie TCP 1443. Ustawienie to można zmienić. Aby można było używać usługi SQL Server Browser do łączenia z wystąpieniami, które nie nasłuchują na domyślnym porcie 1433, potrzebny jest port UDP 1434.
- Domyślnie nazwane wystąpienie programu SQL Server używa portów dynamicznych. Ustawienie to można zmienić.
- Numer portu aktualnie używanego przez aparat bazy danych jest widoczny w dzienniku błędów programu SQL Server. Dzienniki błędów można wyświetlić przy użyciu programu SQL Server Management Studio po połączeniu z nazwanym wystąpieniem. Bieżący dziennik można wyświetlić w obszarze **Zarządzanie — dzienniki SQL Server** w pozycji "serwer nasłuchuje na [" dowolnej "<> IPv4 port_number]".

Musisz włączyć zdalne wywołanie procedury (RPC) na zdalnym wystąpieniu programu SQL Server.

Tryb offline — przepływ pracy kopii zapasowej dla programu DPM

28.02.2020 • 20 minutes to read

Program System Center Data Protection Manager integruje się z Azure Backup i wykorzystuje kilka wbudowanych wydajności, które oszczędzają koszty sieci i magazynowania podczas wstępnej pełnej kopii zapasowej danych na platformie Azure. Wstępne pełne kopie zapasowe zwykle przesyłają duże ilości danych i wymagają większej przepustowości sieci w porównaniu z kolejnymi kopiami zapasowymi, które przesyłają tylko różnice/przyrosty. Azure Backup kompresuje początkowe kopie zapasowe. W procesie umieszczania w trybie offline, Azure Backup mogą używać dysków do przekazywania skompresowanych danych początkowej kopii zapasowej w trybie offline do platformy Azure.

Proces rozsadzenia w trybie offline Azure Backup jest ściśle zintegrowany z [usługą Azure Import/Export](#), która umożliwia transfer danych na platformę Azure przy użyciu dysków. Jeśli masz terabajty (TBs) początkowych danych kopii zapasowej, które muszą być transferowane za pośrednictwem sieci o dużej opóźnieniu i o niskiej przepustowości, możesz użyć przepływu pracy w trybie offline, aby wysłać początkową kopię zapasową na co najmniej jednym dysku twardym do centrum danych platformy Azure. Ten artykuł zawiera omówienie i dalsze szczegóły dotyczące kroków, które uzupełniają ten przepływ pracy dla programu System Center DPM.

NOTE

Proces tworzenia kopii zapasowych w trybie offline dla agenta Microsoft Azure Recovery Services (MARS) różni się od programu System Center DPM. Aby uzyskać informacje na temat korzystania z kopii zapasowej offline z agentem MARS, zobacz [ten artykuł](#). Kopia zapasowa offline nie jest obsługiwana dla kopii zapasowych stanu systemu wykonywanych przy użyciu agenta Azure Backup.

Przegląd

Korzystając z możliwości wypełniania w trybie offline Azure Backup i usługi Azure Import/Export, można łatwo przekazać dane w trybie offline na platformę Azure przy użyciu dysków. Proces tworzenia kopii zapasowej w trybie offline obejmuje następujące kroki:

- Dane kopii zapasowej, które nie są wysyłane przez sieć, są zapisywane w *lokalizacji tymczasowej*
- Dane w *lokalizacji tymczasowej* są następnie zapisywane na jednym lub większej liczbie dysków SATA przy użyciu narzędzia *AzureOfflineBackupDiskPrep*
- Zadanie importowania platformy Azure jest tworzone automatycznie przez narzędzie
- Dyski SATA są następnie wysyłane do najbliższego centrum danych platformy Azure
- Po zakończeniu przekazywania danych kopii zapasowej do platformy Azure Azure Backup kopiuje dane kopii zapasowej do magazynu kopii zapasowych, a przyrostowe kopie zapasowe są zaplanowane.

Wymagania wstępne

Przed zainicjowaniem przepływu pracy tworzenia kopii zapasowej offline upewnij się, że zostały spełnione następujące wymagania wstępne.

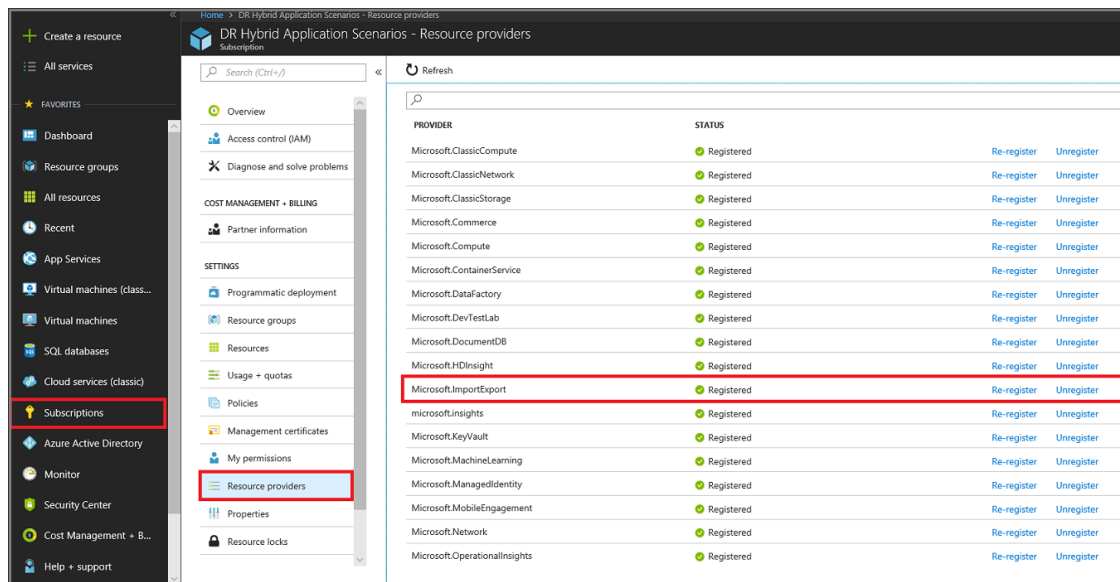
- Utworzono [magazyn Recovery Services](#). Aby go utworzyć, zapoznaj się z instrukcjami w [tym artykule](#).
- Upewnij się, że tylko [Najnowsza wersja agenta Microsoft Azure Recovery Services](#) jest zainstalowana na serwerze SC programu DPM i jest zarejestrowana w magazynie Recovery Services.

- Pakiet zbiorczy aktualizacji 1 jest instalowany na serwerze SC DPM 2019.

NOTE

W przypadku programu DPM 2019 UR1 rozpełnianie w trybie offline przy użyciu Azure Active Directory.

- Na komputerze z uruchomionym agentem Azure Backup upewnij się, że jest zainstalowany program Microsoft Edge lub Internet Explorer 11, a język JavaScript jest włączony.
- Utwórz konto usługi Azure Storage w tej samej subskrypcji co magazyn Recovery Services.
- Upewnij się, że masz odpowiednie [uprawnienia](#) do tworzenia aplikacji Azure Active Directory. Przepływ pracy kopii zapasowej offline tworzy aplikację Azure Active Directory w subskrypcji skojarzonej z kontem usługi Azure Storage. Celem aplikacji jest zapewnienie Azure Backup z bezpiecznym i dostępnym zakresem do usługi Azure import, która jest wymagana dla przepływu pracy kopii zapasowej offline.
- Zarejestruj dostawcę zasobów Microsoft.ImportExport z subskrypcją zawierającą konto usługi Azure Storage. Aby zarejestrować dostawcę zasobów:
 1. W menu głównym kliknij pozycję **subskrypcje**.
 2. Jeśli subskrybujesz wiele subskrypcji, wybierz subskrypcję, która jest używana do tworzenia kopii zapasowych w trybie offline. Jeśli używasz tylko jednej subskrypcji, Twoja subskrypcja zostanie wyświetlona.
 3. W menu subskrypcja kliknij pozycję **dostawcy zasobów**, aby wyświetlić listę dostawców.
 4. Na liście dostawców przewiń w dół do Microsoft.ImportExport. Jeśli stan to NotRegistered, kliknij pozycję **zarejestruj**.



- Tworzona jest lokalizacja tymczasowa, która może być udziałem sieciowym lub dodatkowym dyskiem na komputerze, wewnętrznym lub zewnętrznym, z wystarczającą ilością miejsca na dysku do przechowywania kopii początkowej. Na przykład, jeśli próbujesz utworzyć kopię zapasową serwera plików 500-GB, upewnij się, że obszar przejściowy jest co najmniej 500 GB. (Mniejsza ilość jest używana z powodu kompresji).
- W odniesieniu do dysków, które będą wysyłane do platformy Azure, należy się upewnić, że używane są tylko dyski SSD 2,5 cala lub 2,5 cala lub 3,5 cala SATA II/III. Możesz użyć dysków twardych o pojemności do 10 TB. Zapoznaj się z [dokumentacją usługi Azure Import/Export](#), aby zapoznać się z najnowszym zestawem dysków obsługiwanych przez usługę.
- Dyski SATA muszą być połączone z komputerem (nazywanym *komputerem kopiującym*), z którego są

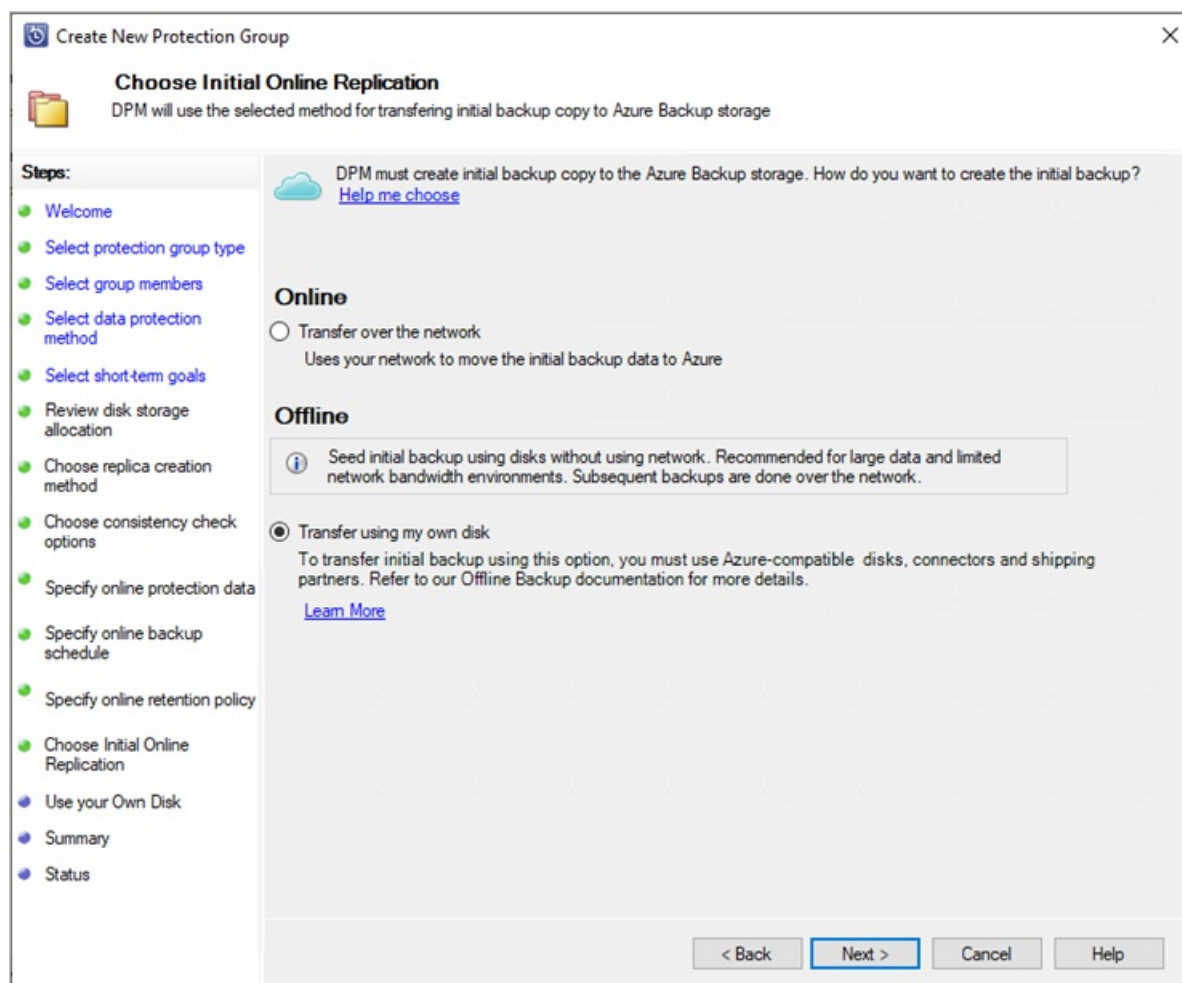
wykonywane kopie kopii zapasowych z *lokalizacji tymczasowej* do dysków SATA. Upewnij się, że funkcja BitLocker jest włączona na *komputerze kopiowania*

Przepływ pracy

Informacje przedstawione w tej sekcji ułatwiają zakończenie przepływu pracy w trybie offline, aby dane mogły zostać dostarczone do centrum danych platformy Azure i przekazane do usługi Azure Storage. Jeśli masz pytania dotyczące usługi import lub dowolnego aspektu procesu, zapoznaj się z dokumentacją dotyczącą [przeglądu usługi Import Service](#).

Inicjowanie kopii zapasowej offline

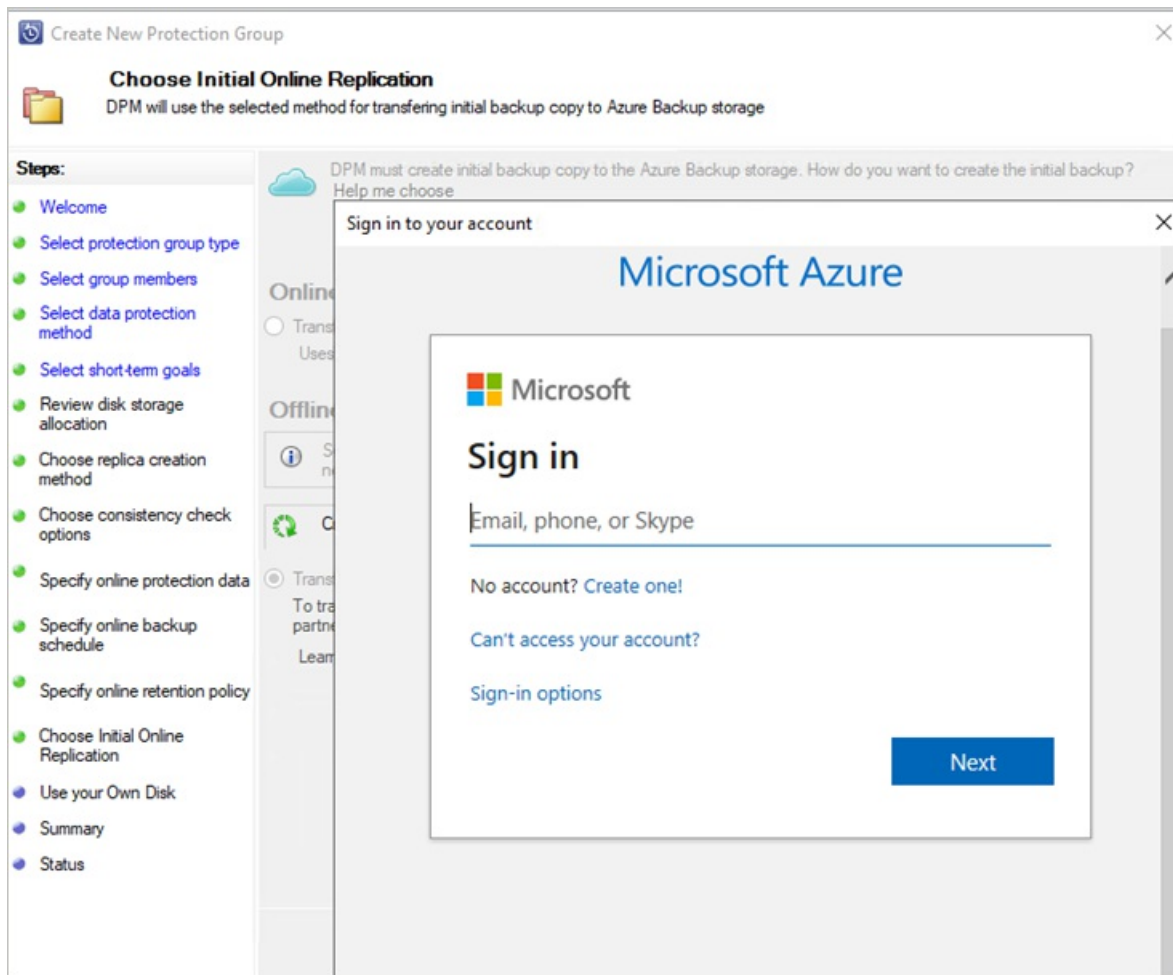
1. Po utworzeniu nowej grupy ochrony z ochroną w trybie online lub dodaniu ochrony w trybie online do istniejącej grupy ochrony zostanie wyświetlony poniższy ekran. Aby wybrać metodę początkowej replikacji online, wybierz pozycję **transfer przy użyciu własnego dysku** i kliknij przycisk **dalej**.



NOTE

W przypadku zbiorczego aktualizowania programu DPM 2019 w przypadku wybrania opcji **Dodaj ochronę w trybie online** dla istniejącej grupy ochrony może się zdarzyć, że konsola. Aby rozwiązać ten problem, Zastosuj poprawkę zgodnie z opisem w [artykule KB](#).

2. Zostanie otwarta strona logowania platformy Azure. Zaloguj się przy użyciu konta użytkownika platformy Azure, które ma uprawnienia roli *właściciela* w ramach subskrypcji platformy Azure.



3. Podaj dane wejściowe na stronie **Korzystanie z własnego dysku**.

Opis danych wejściowych jest następujący:

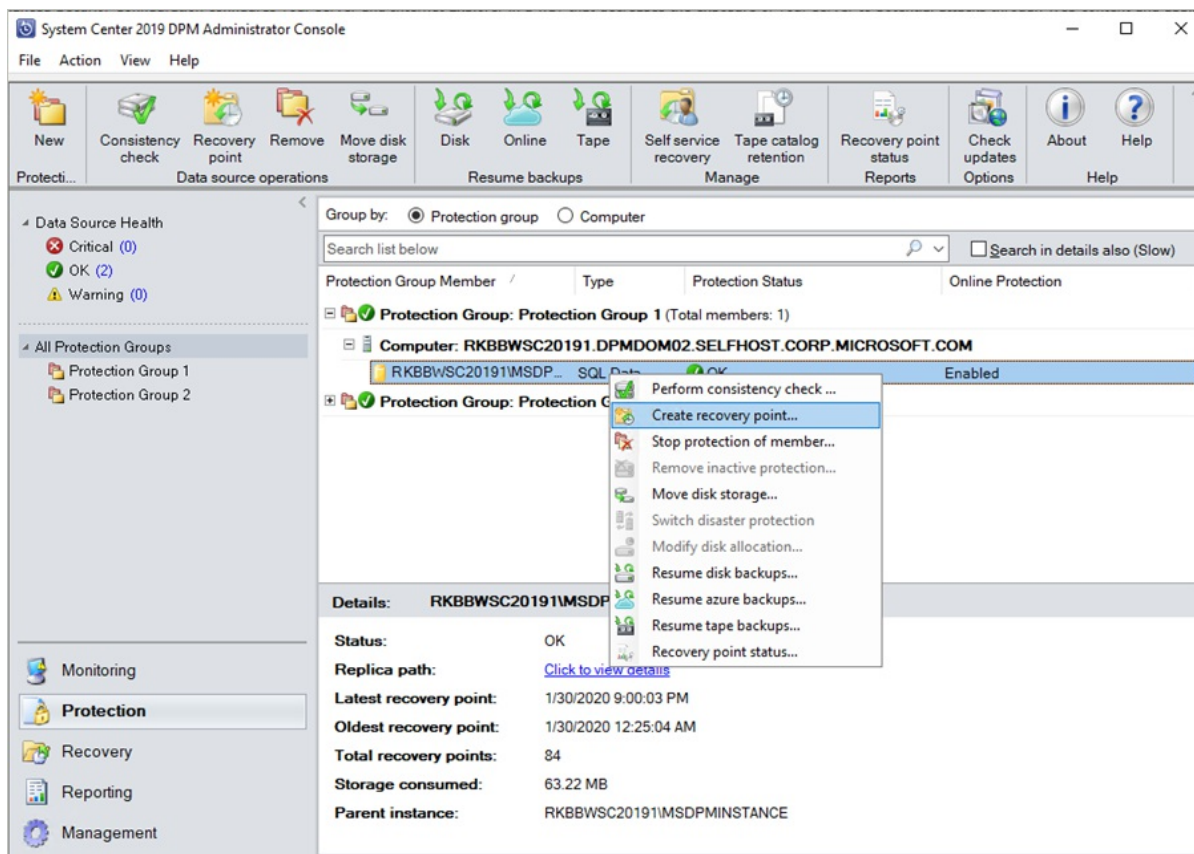
- **Lokalizacja tymczasowa:** tymczasowa lokalizacja przechowywania, w której zapisano początkową kopię zapasową. Lokalizacja przejściowa może znajdować się w udziale sieciowym lub na komputerze lokalnym. Jeśli komputer kopii i komputer źródłowy są inne, zalecamy określenie pełnej ścieżki

sieciowej lokalizacji tymczasowej.

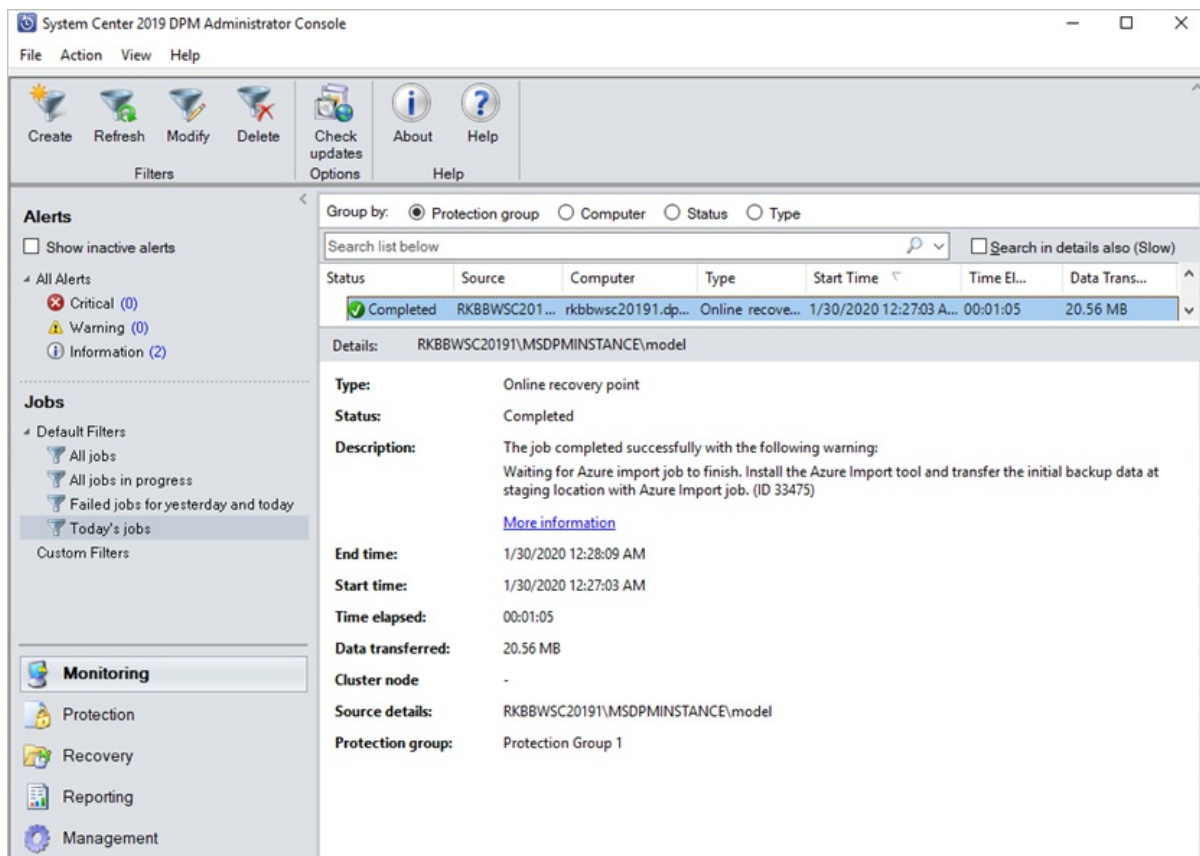
- **Konto usługi Azure Storage:** nazwa konta magazynu w subskrypcji platformy Azure skojarzona z plikiem ustawień publikowania platformy Azure.
- **Kontener usługi Azure Storage:** Nazwa docelowego obiektu blob magazynu na koncie usługi Azure Storage, do którego są importowane dane kopii zapasowej.
- **Identyfikator subskrypcji platformy Azure:** Identyfikator subskrypcji platformy Azure dla subskrypcji z lokalizacji, w której pobrano plik ustawień publikowania platformy Azure.
- **Nazwa zadania importowania platformy Azure:** unikatowa nazwa, za pomocą której usługa Azure Import i Azure Backup śledzi transfer danych wysyłanych na dyskach na platformę Azure.

Zapisz lokalizację przemieszczania i nazwę zadania importowania platformy Azure podane jako wymagane do przygotowania dysków.

4. Ukończ przepływ pracy, aby utworzyć lub zaktualizować ochronę. Aby zainicjować kopię zapasową offline, kliknij prawym przyciskiem myszy **grupę ochrony**, a następnie wybierz opcję **Utwórz punkt odzyskiwania** . Następnie wybierz opcję **ochrony w trybie online** .



5. Monitoruj zadanie tworzenia repliki online w okienku Monitorowanie. Zadanie powinno zostać wykonane pomyślnie, a ostrzeżenie *oczekuje na zakończenie zadania importowania platformy Azure*.



6. Po zakończeniu operacji lokalizacja tymczasowa jest gotowa do użycia podczas przygotowywania dysku.

Przygotowanie dysków SATA i dostarczenie do platformy Azure

Narzędzie *AzureOfflineBackupDiskPrep* przygotowuje dyski SATA, które są wysyłane do najbliższego centrum danych platformy Azure. To narzędzie jest dostępne w katalogu instalacji agenta Azure Backup (w następującej ścieżce):

```
*\Microsoft Azure Recovery Services Agent\Utils\*
```

1. Przejdź do katalogu i Skopiuj katalog **AzureOfflineBackupDiskPrep** do innego komputera, na którym są połączone stacje dysków SATA. Na komputerze z podłączonymi dyskami SATA upewnij się, że:

- Komputer kopii może uzyskać dostęp do lokalizacji tymczasowej przepływu pracy w trybie offline przy użyciu tej samej ścieżki sieciowej, która została podana w przepływie pracy **inicjowania kopii zapasowej offline**.
- Funkcja BitLocker jest włączona na komputerze kopiowania.
- Program Azure PowerShell 3.7.0 jest instalowany na komputerze z kopią (nie jest to wymagane, jeśli na serwerze programu DPM jest uruchomione narzędzie AzureOfflineBackupDiskPrep).
- Są zainstalowane najnowsze zgodne przeglądarki (Microsoft Edge lub Internet Explorer 11), a język JavaScript jest włączony.
- Komputer kopiowania może uzyskać dostęp do Azure Portal. W razie potrzeby komputer kopii może być taki sam jak komputer źródłowy.

IMPORTANT

Jeśli komputer źródłowy jest maszyną wirtualną, komputer do kopiowania musi być innym serwerem fizycznym lub komputerem klienckim z komputera źródłowego.

2. Otwórz wiersz polecenia z podwyższonym poziomem uprawnień na komputerze kopiowania przy użyciu katalogu narzędzi *AzureOfflineBackupDiskPrep* jako bieżący katalog i uruchom następujące polecenie:

```
.\AzureOfflineBackupDiskPrep.exe s:<Staging Location Path>
```

PARAMETR	DESCRIPTION
s:<ścieżka lokalizacji tymczasowej>	Obowiązkowe dane wejściowe używane do zapewnienia ścieżki do lokalizacji tymczasowej wprowadzonej w przepływie pracy inicjowania kopii zapasowej offline .
p:<ścieżka do PublishSettingsFile>	Opcjonalne dane wejściowe używane do zapewnienia ścieżki do pliku ustawień publikowania platformy Azure wprowadzonego w przepływie pracy inicjowania kopii zapasowej offline .

Po uruchomieniu polecenia Narzędzie żąda wyboru zadania importowania platformy Azure odpowiadającego dyskom, które muszą zostać przygotowane. Jeśli tylko jedno zadanie importu jest skojarzone z podaną lokalizacją przemieszczania, zobaczysz ekran podobny do poniższego.

```
Administrator: Command Prompt
C:\Program Files\Microsoft Azure Recovery Services Agent\Utils\AzureOfflineBackupDiskPrep>AzureOfflineBackupDiskPrep.exe s:C:\StagingLocation
Parsed input parameters successfully.
Session Started
Current Directory : C:\Program Files\Microsoft Azure Recovery Services Agent\Utils\AzureOfflineBackupDiskPrep
Tool Directory : C:\Program Files\Microsoft Azure Recovery Services Agent\Utils\AzureOfflineBackupDiskPrep\
Journal file name : Journalf2b9c555-fa03-434c-bebe-09e11edd69c0.jrn

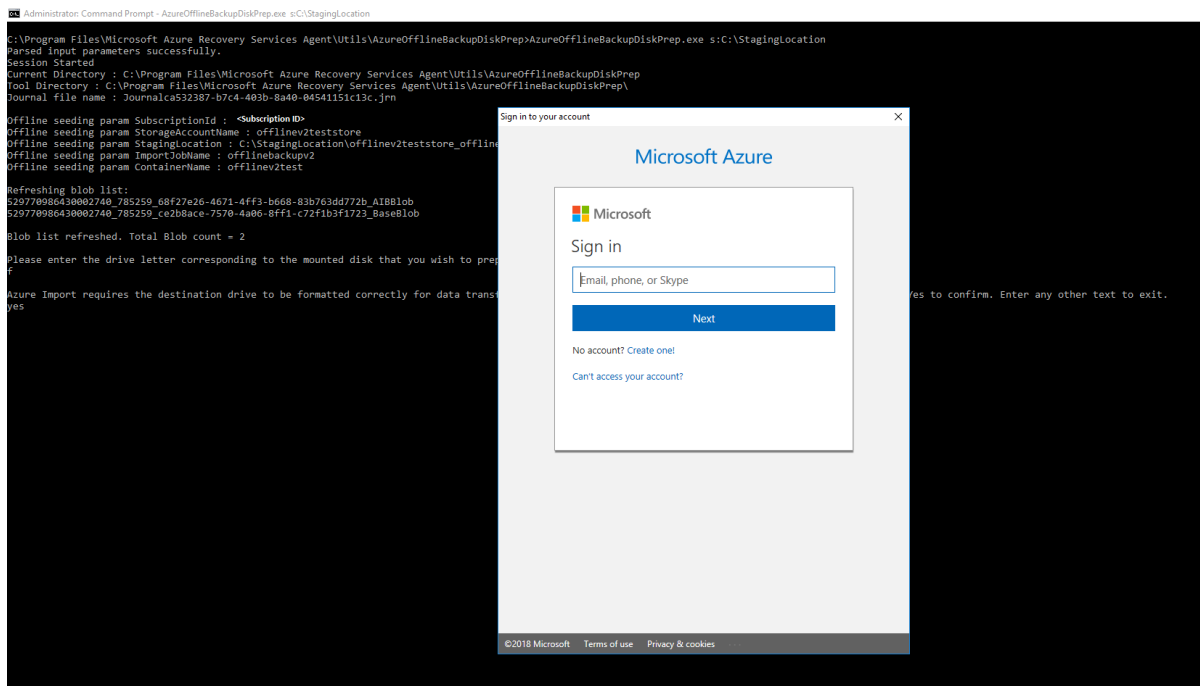
Offline seeding param SubscriptionId : <Subscription ID>
Offline seeding param StorageAccountName : offlinev2teststore
Offline seeding param StagingLocation : C:\StagingLocation\offlinev2teststore_offlinebackupv2
Offline seeding param ImportJobName : offlinebackupv2
Offline seeding param ContainerName : offlinev2test

Refreshing blob list:
529770986430002740_785259_68f27e26-4671-4ff3-b668-83b763dd772b_AI8B10b
529770986430002740_785259_ce2b8ace-7570-4a06-8ff1-c72f1b3f1723_Base10b

Blob list refreshed. Total Blob count = 2

Please enter the drive letter corresponding to the mounted disk that you wish to prepare.
F
```

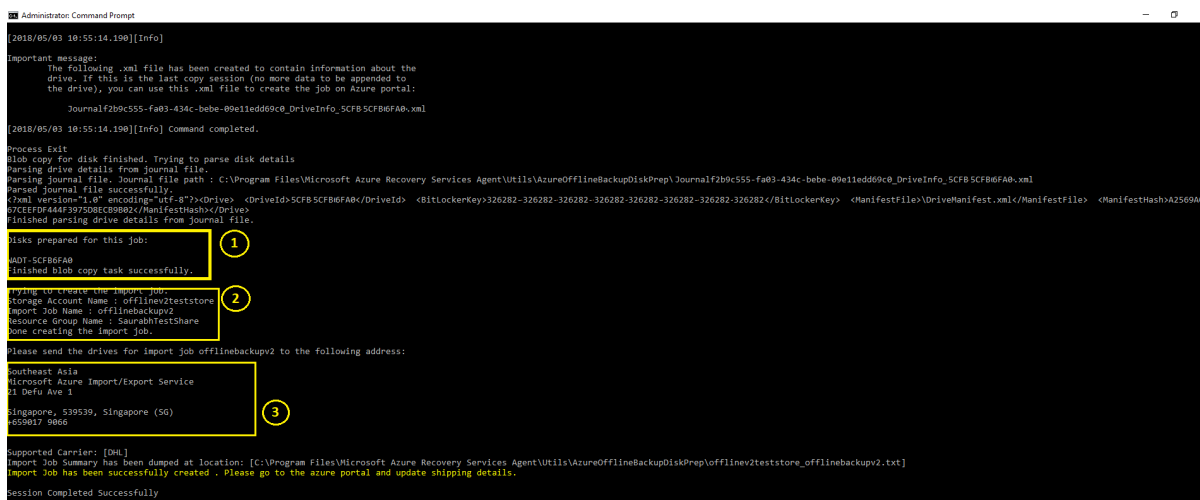
3. Wprowadź literę dysku bez kropki końcowej dla zainstalowanego dysku, który ma zostać przygotowany do przeniesienia na platformę Azure.
4. Potwierdź formatowanie dysku po wyświetleniu monitu.
5. Zostanie wyświetlony monit o zalogowanie się do subskrypcji platformy Azure. Wprowadź swoje poświadczenia.



Następnie narzędzie rozpocznie przygotowanie dysku i skopiowanie danych kopii zapasowej. W przypadku, gdy udostępniony dysk nie ma wystarczającej ilości miejsca na dane kopii zapasowej, może być konieczne dołączenie dodatkowych dysków.

Po pomyślnym wykonaniu tego narzędzia wiersz polecenia zawiera trzy informacje:

- Co najmniej jeden z podanych dysków jest przygotowywany do wysyłania do platformy Azure.
- Otrzymasz potwierdzenie, że zadanie importowania zostało utworzone. Zadanie importowania używa podanej nazwy.
- Narzędzie wyświetla adres wysyłkowy centrum danych platformy Azure.



6. Po zakończeniu wykonywania polecenia można zaktualizować informacje o wysyłce.
7. Wyślij dyski na adres dostarczony przez narzędzie i Zachowaj numer śledzenia na potrzeby przyszłego odwołania.

IMPORTANT

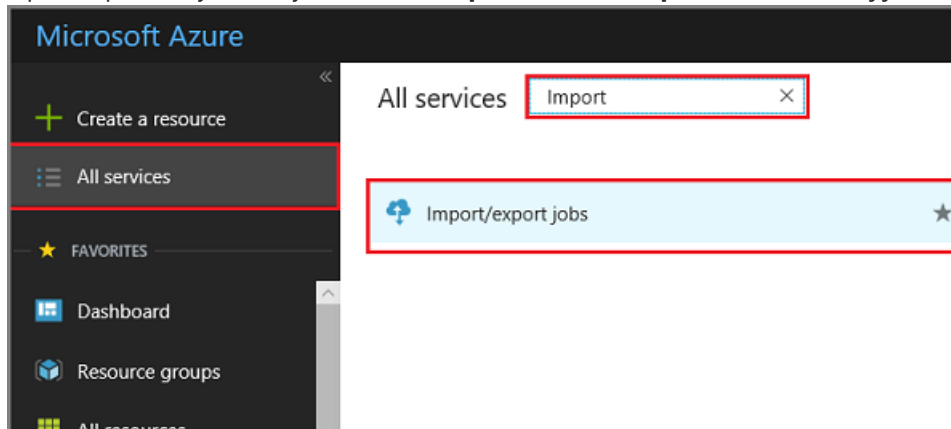
Żadne dwa zadania importowania platformy Azure nie mogą mieć tego samego numeru śledzenia. Upewnij się, że dyski przygotowane przez narzędzie w ramach pojedynczego zadania importowania platformy Azure są dostarczane razem w jednym pakiecie i że istnieje jeden unikatowy numer śledzenia dla pakietu. Nie łącz dysków przygotowanych w ramach oddzielnych zadań importowania platformy Azure w jednym pakiecie.

Aktualizowanie szczegółów wysyłki w ramach zadania importowania platformy Azure

Poniższa procedura umożliwi zaktualizowanie informacji o wysyłce zadania importowania platformy Azure. Informacje te zawierają szczegółowe informacje na temat:

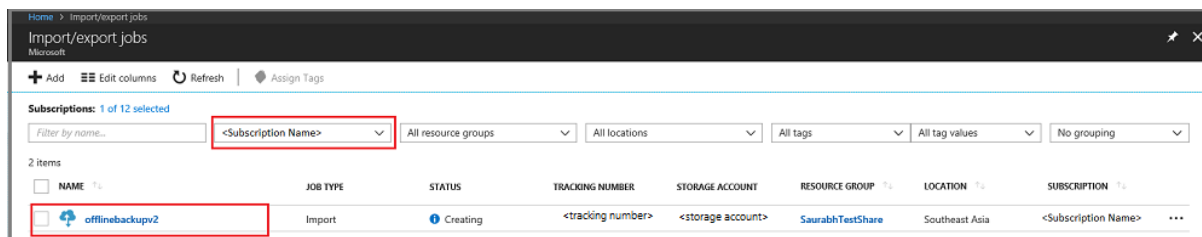
- Nazwa przewoźnika, który dostarcza dyski do platformy Azure
- Zwróć szczegóły dotyczące wysyłki dla dysków

1. Zaloguj się do subskrypcji platformy Azure.
2. W menu głównym kliknij pozycję **wszystkie usługi**, a następnie w oknie dialogowym wszystkie usługi wpisz import. Gdy zobaczysz **zadania importowania/eksportowania**, kliknij je.



Zostanie otwarta lista **zadań Importuj/Eksportuj zadania** i zostanie wyświetlona lista wszystkich zadań importu/eksportu w wybranej subskrypcji.

3. Jeśli masz wiele subskrypcji, pamiętaj o wybraniu subskrypcji użytej do zaimportowania danych kopii zapasowej. Następnie wybierz nowo utworzone zadanie importu, aby otworzyć jego szczegóły.



4. W menu Ustawienia zadania importowania kliknij pozycję **Zarządzaj informacjami o wysyłce**, a następnie wprowadź szczegóły dotyczące wysyłki zwrotnej.

Microsoft Azure

Home > Import/export jobs > offlinebackupv2 - Manage shipping info

offlinebackupv2 - Manage shipping info

Import/export job

Search (Ctrl+F)

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

SETTINGS

Manage shipping info

BitLocker keys

Properties

Locks

Automation script

MONITORING

Diagnostics

SUPPORT + TROUBLESHOOTING

New support request

Save Discard

Return carrier

* Carrier name

DHL

* Carrier account number

34134832

Return address

* Contact name

Administrator

* Phone

2431313312

* Email

admin@contoso.com

* Street address 1

Contoso One, Building Zero, Park Street

Street address 2 (optional)

* City

Hyderabad

* Zip code

500072

State/Province

Telangana

* Country/Region

India

5. Jeśli numer śledzenia jest używany przez firmę wysyłkową, kliknij transparent na stronie Przegląd zadania importowania platformy Azure i wprowadź następujące informacje:

IMPORTANT

Upewnij się, że informacje o przewoźniku i numer śledzenia zostały zaktualizowane w ciągu dwóch tygodni od utworzenia zadania importowania platformy Azure. Niepowodzenie weryfikacji tych informacji w ciągu dwóch tygodni może skutkować usunięciem zadania i nieprzetwarzaniem dysków.

Microsoft Azure

Report a bug

Search resources, services, and docs

offlinebackupv2

Import/export job

Search (Ctrl+F)

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

SETTINGS

Manage shipping info

BitLocker keys

Properties

Locks

Automation script

MONITORING

Diagnostics

SUPPORT + TROUBLESHOOTING

New support request

Cancel job Move Delete

For job to progress, provide the tracking information. The job will be deleted if tracking information is not updated within 2 weeks of job creation

Essentials

Resource group (change)

SaurabhTestShare

Status

Creating

Location

Southeast Asia

Subscription name (change)

<Subscription

Subscription ID

<Subscription ID>

Overall percent completed

-

Storage account

offlinev2teststore

Type

Import

Delivery tracking number

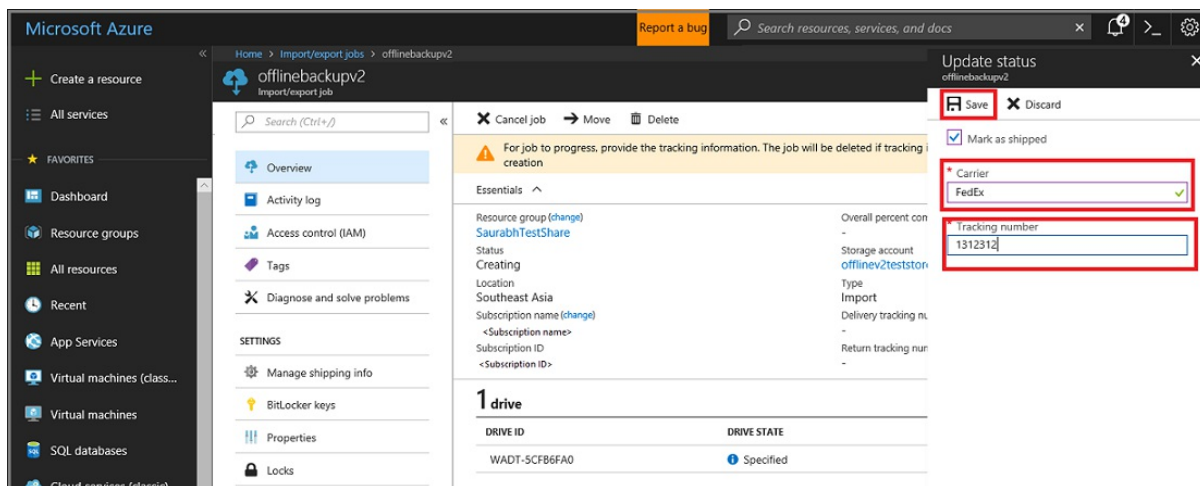
-

Return tracking number

-

1 drive

DRIVE ID	DRIVE STATE	PERCENT COMPLETE
WADT-5CFB6FA0	Specified	-



Czas do przetworzenia dysków

Czas przetwarzania zadania importowania platformy Azure zależy od różnych czynników, takich jak czas wysyłki, typ zadania, typ i rozmiar kopiowanych danych oraz rozmiar udostępnionych dysków. Usługa Azure Import/Export nie ma umowy SLA, ale po odebraniu dysków usługa dokłada starań, aby zakończyć kopiowanie danych kopii zapasowej na konto usługi Azure Storage w ciągu 7 do 10 dni. W następnej sekcji szczegółowo opisano, jak można monitorować stan zadania importowania platformy Azure.

Monitorowanie stanu zadania importowania platformy Azure

Stan zadania importowania można monitorować z Azure Portal, przechodząc do strony **Importuj/Eksportuj zadania** i wybierając zadanie. Aby uzyskać więcej informacji na temat stanu zadań importowania, zobacz artykuł [Magazyn importu usługi Export](#).

Ukończ przepływ pracy

Po zakończeniu zadania importowania dane początkowej kopii zapasowej są dostępne na koncie magazynu. W czasie następnej zaplanowanej kopii zapasowej usługa Azure Backup kopiuje zawartość danych z konta magazynu do magazynu Recovery Services.

Podczas następnego zaplanowanego zadania tworzenia repliki w trybie online Data Protection Manager wykonuje przyrostową kopię zapasową za pomocą początkowej kopii zapasowej.

Następne kroki

- Aby uzyskać odpowiedzi na pytania dotyczące przepływu pracy importowania/eksportowania platformy Azure, zapoznaj się z tematem [transfer danych do magazynu obiektów BLOB za pomocą usługi Microsoft Azure Import/Export](#).

Tworzenie kopii zapasowych maszyn wirtualnych funkcji Hyper-V

11.12.2019 • 48 minutes to read

Program System Center Data Protection Manager (DPM) chroni maszyny wirtualne funkcji Hyper-V przez tworzenie kopii zapasowych danych maszyny wirtualnej. Możesz wykonać kopię zapasową danych na poziomie hosta funkcji Hyper-V, aby włączyć odzyskiwanie danych na poziomie maszyny wirtualnej i na poziomie pliku, lub wykonać kopię zapasową na poziomie gościa, aby włączyć odzyskiwanie na poziomie aplikacji.

Scenariusze obsługiwane

Program DPM może wykonywać kopie zapasowe maszyn wirtualnych działających na serwerach hostów funkcji Hyper-V w następujących scenariuszach:

- **Maszyny wirtualne z magazynem lokalnym lub podłączonym bezpośrednio** — wykonywanie kopii zapasowych maszyn wirtualnych hostowanych na autonomicznych serwerach hosta funkcji Hyper-V mających lokalną lub podłączoną bezpośrednio pamięć masową. Na przykład dysk twardy, urządzenie sieci SAN lub urządzenie sieciowej pamięci masowej (NAS). Agent ochrony programu DPM musi być zainstalowany na wszystkich hostach.
- **Maszyny wirtualne w klastrze z magazynem CSV** — wykonywanie kopii zapasowych maszyn wirtualnych hostowanych w klastrze funkcji Hyper-V z woluminem udostępnionym klastra (CSV). W wersji DPM 2012 SP1 wprowadzono ekspresowe pełne kopie zapasowe, równoległe kopie zapasowe i usprawnienia zapytań klastra dla kopii zapasowych woluminów udostępnionych klastra. Agent ochrony DPM jest instalowany na każdym węźle klastra.
- **Maszyny wirtualne z magazynem SMB** — wykonywanie kopii zapasowych maszyn wirtualnych hostowanych na serwerze autonomicznym lub klastrze funkcji Hyper-V z serwerem plików SMB 3.0. Obsługiwane są udziały SMB na autonomicznym serwerze plików lub klastrze serwerów plików. Jeśli używasz zewnętrznego serwera plików SMB 3.0, powinien być na nim zainstalowany agent ochrony programu DPM. Jeśli serwer pamięci masowej jest klastrowany, agent powinien być zainstalowany na każdym węźle klastra. Konto machine\$ serwera aplikacji musi mieć uprawnienia do całego udziału i na poziomie folderów na udziale SMB.
- **Kopia zapasowa maszyn wirtualnych skonfigurowanych do migracji na żywo** — migracja na żywo umożliwia przenoszenie maszyn wirtualnych z jednej lokalizacji do innej, zapewniając jednocześnie niezakłócony dostęp. Możesz przenosić maszyny wirtualne między dwoma serwerami autonomicznymi wewnątrz jednego klastra lub między serwerami autonomicznymi i węzłami klastra. Jednocześnie można uruchomić wiele migracji na żywo. Istnieje również możliwość migracji na żywo magazynu maszyn wirtualnych, aby przenieść maszyny do nowych lokalizacji przechowywania bez przerywania ich działania. Program DPM może wykonywać kopie zapasowe maszyn wirtualnych skonfigurowanych do migracji na żywo. Przeczytaj więcej.
- **Kopia zapasowa maszyn wirtualnych repliki** — wykonywanie kopii zapasowej maszyn wirtualnych repliki działających na serwerze pomocniczym (tylko DPM 2012 R2)

Dowiedz się więcej na temat obsługiwanych wersji programu DPM i funkcji Hyper-V w temacie [What can DPM back up?](#) (Co program DPM może umieścić w kopii zapasowej?) .

Kopia zapasowa hosta a kopia zapasowa gościa

Program DPM może wykonywać kopie zapasowe maszyn wirtualnych funkcji Hyper-V na poziomie hosta lub gościa. Na poziomie hosta agent ochrony programu DPM jest zainstalowany na serwerze lub klastrze hosta funkcji Hyper-V i chroni wszystkie maszyny wirtualne oraz pliki danych działające na tym hoście. Na poziomie gościa agent jest zainstalowany na każdej maszynie wirtualnej i chroni obciążenie obecne na tej maszynie.

Obie metody mają swoje zalety i wady:

- Kopie zapasowe na poziomie hosta są elastyczne, ponieważ działają niezależnie od rodzaju systemu operacyjnego funkcjonującego na maszynach gościa i nie wymagają instalacji agenta ochrony programu DPM na każdej maszynie wirtualnej. W przypadku wdrożenia kopii zapasowej na poziomie hosta możliwe będzie odzyskanie całej maszyny wirtualnej lub plików i folderów (odzyskiwanie na poziomie elementu).
- Kopia zapasowa na poziomie gościa jest przydatna do ochrony konkretnych zadań działających na maszynie wirtualnej. Na poziomie hosta można odzyskać całą maszynę wirtualną lub określone pliki, ale niemożliwe jest odzyskiwanie w kontekście określonej aplikacji. Aby na przykład można było odzyskać określone elementy programu SharePoint z kopii zapasowej maszyny wirtualnej, należy wykonać kopię zapasową tej maszyny wirtualnej na poziomie gościa. Pamiętaj, że do ochrony danych znajdujących się na dyskach przekazujących należy używać kopii zapasowej na poziomie gościa. Przekazywanie umożliwia maszynie wirtualnej bezpośredni dostęp do urządzenia pamięci masowej bez przechowywania danych woluminu wirtualnego w pliku VHD.

Kopia zapasowa w trybie online i w trybie offline

IMPORTANT

W zależności od konfiguracji programu DPM i ochrony kopii zapasowych w trybie online i w trybie offline program DPM różni się od siebie. Jeśli używasz programu DPM 2012 R2 z UR3 (lub nowszego) do ochrony funkcji Hyper-V w systemie Windows Server 2012 R2 (lub nowszym), maszyny wirtualne kontynuują działanie podczas tworzenia kopii zapasowej. W takim przypadku pozostała część tej sekcji nie ma zastosowania.

W przypadku ochrony serwera funkcji Hyper-V w systemie Windows Server 2012 lub w przypadku korzystania z programu DPM 2012 R2 z UR1 lub UR2, Następująca sekcja ma zastosowanie do konfiguracji:

Program DPM bezproblemowo współdziała z modułem zapisywania usług kopiowania woluminów w tle (VSS) funkcji Hyper-V, aby zapewnić przechwycenie i ochronę spójnych wersji maszyn wirtualnych bez wpływu na dostęp do maszyny wirtualnej. Możliwość tworzenia kopii zapasowej otwartych plików jest kluczowa dla ciągłości działania. Domyślnie program DPM wykonuje kopie zapasowe online, które nie wpływają na dostępność maszyn wirtualnych. Wykonywanie kopii zapasowych online ma następujące wymagania:

- Musi być włączona usługa integracji wykonywania kopii zapasowych, więc system operacyjny na maszynie wirtualnej musi obsługiwać usługi integracji funkcji Hyper-V.
- System operacyjny gościa musi obsługiwać usługi VSS (Windows Server 2003 lub nowszy). Nie jest obsługiwane wykonywanie kopii zapasowej online, gdy na maszynach wirtualnych działa system Linux.
- Maszyna wirtualna nie powinna mieć żadnych dysków dynamicznych.
- Wszystkie woluminy muszą mieć system plików NTFS
- Nie można modyfikować przydziału magazynu usług VSS dla woluminów.
- Maszyna wirtualna musi być uruchomiona, a jeśli maszyna wirtualna jest w klastrze, grupa zasobów klastra powinna być w trybie online. Przypisanie magazynu kopii w tle woluminu w maszynie wirtualnej nie może być jawnie ustawione na inny wolumin.

Jeśli te warunki nie będą spełnione, program DPM będzie wykonywać kopie zapasowe offline, czyli wstrzymywać maszynę wirtualną i przełączać ją do zapisanego stanu na czas wykonywania migawki, a następnie wznawiać jej

działanie. Oznacza to, że maszyna wirtualna jest niedostępna podczas wykonywania kopii zapasowej, zwykle krócej niż minutę w wielu środowiskach.

Jak działa proces tworzenia kopii zapasowej

Program DPM wykonuje kopię zapasową z usługami VSS w następujący sposób. Kroki znajdujące się w tym opisie są ponumerowane w celu zwiększenia przejrzystości.

1. Aparat synchronizacji opartej na blokach programu DPM tworzy początkową kopię chronionej maszyny wirtualnej i zapewnia kompletność oraz spójność tej kopii.
2. Po utworzeniu i sprawdzeniu kopii początkowej program DPM korzysta ze składnika zapisywania usługi VSS funkcji Hyper-V do przechwytywania kopii zapasowych. Składnik zapisywania usługi VSS dostarcza zestaw bloków dysków ze spójnymi danymi, które są synchronizowane z serwerem programu DPM. Metoda ta umożliwia tworzenie „pełnej kopii zapasowej” przy użyciu serwera programu DPM, ograniczając jednocześnie ilość danych kopii zapasowej, które muszą zostać przesłane przez sieć.
3. Agent ochrony programu DPM na serwerze z uruchomioną funkcją Hyper-V ustala przy użyciu interfejsów API funkcji Hyper-V, czy chroniona maszyna wirtualna również obsługuje usługę VSS.

- Jeśli maszyna wirtualna spełnia wymagania kopii zapasowej online i ma zainstalowany składnik usług integracji funkcji Hyper-V, to element zapisujący usług VSS funkcji Hyper-V rekursywnie przekazuje żądania usług VSS do wszystkich procesów obsługujących takie żądania na maszynie wirtualnej. Ta operacja odbywa się bez konieczności instalowania na maszynie wirtualnej agenta ochrony programu DPM. Dzięki tym cyklicznym żądaniom składnik zapisywania usługi VSS funkcji Hyper-V może się upewnić, że operacje zapisu na dysku są zsynchronizowane, aby przechwycić migawkę usługi VSS bez utraty danych.

Składnik usług integracji funkcji Hyper-V wywołuje składnik zapisywania usługi VSS funkcji Hyper-V w ramach usług kopiowania woluminów w tle (VSS) w maszynach wirtualnych, aby sprawdzić, czy dane aplikacji są spójne.

- Jeśli maszyna wirtualna nie spełnia wymagań kopii zapasowej online, program DPM przy użyciu interfejsu API funkcji Hyper-V automatycznie wstrzymuje maszynę wirtualną przed przechwyceniem plików danych.
4. Po zsynchronizowaniu początkowej, podstawowej kopii maszyny wirtualnej z serwerem programu DPM wszystkie zmiany wprowadzone w zasobach maszyny wirtualnej są przechwytywane do nowego punktu odzyskiwania. Punkt odzyskiwania przedstawia stan spójności maszyny wirtualnej w określonym czasie. Przechwytywanie w ramach punktu odzyskiwania może odbywać się co najmniej raz dziennie. Po utworzeniu nowego punktu odzyskiwania program DPM ustala przy użyciu replikacji na poziomie bloku w połączeniu ze składnikiem zapisywania usługi VSS funkcji Hyper-V, które bloki zostały zmienione na serwerze z uruchomioną funkcją Hyper-V od ostatniego utworzenia punktu odzyskiwania. Te bloki danych zostają następnie przetransferowane na serwer programu DPM i zastosowane do repliki chronionych danych.
 5. Serwer programu DPM korzysta z usług VSS na woluminach hostujących dane odzyskiwania, dzięki czemu dostępnych jest wiele kopii w tle. Każda z tych kopii w tle zapewnia osobne zadania odzyskiwania. Punkty odzyskiwania usługi VSS są przechowywane na serwerze programu DPM. Kopia tymczasowa utworzona na serwerze z uruchomioną funkcją Hyper-V jest przechowywana tylko przez czas synchronizacji z programem DPM.

Wymagania wstępne dotyczące kopii zapasowej

Oto wymagania wstępne dotyczące tworzenia kopii zapasowych maszyn wirtualnych funkcji Hyper-V za pomocą programu DPM.

WYMAGANIE WSTĘPNE	SZCZEGÓŁY
Wymagania wstępne programu DPM	— Jeśli chcesz przeprowadzić odzyskiwanie na poziomie elementu dla maszyn wirtualnych (odzyskanie plików, folderów, woluminów), musisz zainstalować rolę funkcji Hyper-V na serwerze programu DPM. Jeśli chcesz tylko odzyskać maszynę wirtualną i nie schodzić do poziomu elementów, ta rola nie jest wymagana. — Możesz chronić do 800 maszyn wirtualnych (każda z nich może zawierać 100 GB) na jednym serwerze programu DPM i stosować wiele serwerów programu DPM obsługujących większe klastry. — W celu zwiększenia wydajności tworzenia kopii zapasowych maszyn wirtualnych program DPM pomija plik stronicowania podczas tworzenia przyrostowych kopii zapasowych. — Program DPM może wykonywać kopie zapasowe serwera lub klastra funkcji Hyper-V w tej samej domenie, w której znajduje się serwer programu DPM, lub w podrzędnej lub zaufanej domenie. Jeśli chcesz wykonywać kopie zapasowe serwera funkcji Hyper-V w grupie roboczej lub w niezaufanej domenie, musisz skonfigurować uwierzytelnianie. W przypadku pojedynczego serwera funkcji Hyper-V możesz użyć uwierzytelniania NTLM lub uwierzytelniania opartego na certyfikacie. W przypadku klastra możesz użyć tylko uwierzytelniania opartego na certyfikacie. — Przy tworzeniu kopii zapasowej danych maszyny wirtualnej na dyskach przekazujących nie jest obsługiwane korzystanie z kopii zapasowych na poziomie hosta. W tym scenariuszu firma Microsoft zaleca użycie kopii zapasowej na poziomie hosta do wykonywania kopii zapasowej plików VHD, zaś kopie zapasowe na poziomie gościa powinny być używane do tworzenia kopii zapasowych innych danych, które nie są widoczne na hoście. — Podczas ochrony klastra funkcji Hyper-V za pomocą skalowanej w poziomie ochrony programu DPM (wiele serwerów DPM chroniących duży klaster funkcji Hyper-V) nie można dodać dodatkowej ochrony dla chronionych obciążeń funkcji Hyper-V. — Kopię zapasową maszyn wirtualnych repliki można utworzyć tylko wtedy, gdy program DPM działa w programie System Center 2012 R2 i host funkcji Hyper-V jest uruchomiony w systemie Windows Server 2012 R2. — Można utworzyć kopię zapasową woluminów deduplikowanych.

WYMAGANIE WSTĘPNE	SZCZEGÓŁY
Wymagania wstępne maszyny wirtualnej funkcji Hyper-V	— Wersja składników integracji uruchamiana na maszynie wirtualnej powinna być taka sama jak wersja funkcji Hyper-V na serwerze z działającą funkcją Hyper-V. — Dla każdej kopii zapasowej maszyny wirtualnej będzie wymagane wolne miejsce na woluminie obsługującym pliki wirtualnego dysku twardego, aby dostarczyć funkcji Hyper-V wystarczającą ilość miejsca na dyski różnicowe (AVHD) podczas wykonywania kopii zapasowej. Ilość miejsca musi wynosić co najmniej tyle, ile wynosi obliczona wartość początkowy rozmiar dysku *tempo zmian* okno czasu wykonywania kopii zapasowej. Jeśli używasz wielu kopii zapasowych w klastrze, konieczna będzie obliczona w ten sposób wystarczająca ilość miejsca do magazynowania dysków AVHD dla poszczególnych maszyn wirtualnych. — Jeśli chcesz tworzyć kopie zapasowe maszyn wirtualnych znajdujących się na serwerach hostów funkcji Hyper-V z systemem Windows Server 2012 R2, maszyna wirtualna powinna mieć zdefiniowany kontroler SCSI, nawet jeśli nie jest podłączona do żadnego elementu. Jest tak, ponieważ podczas tworzenia kopii zapasowej online w systemie Windows Server 2012 R2 host funkcji Hyper-V instaluje nowy wirtualny dysk twardy w maszynie wirtualnej i później odinstalowuje go. Te operacje mogą być obsługiwane wyłącznie przez kontroler SCSI i dlatego takie wymaganie obowiązuje w przypadku kopii zapasowej online maszyny wirtualnej. To wyjaśnia, dlaczego jest potrzebny kontroler SCSI. Bez tego ustawienia podczas próby utworzenia kopii zapasowej maszyny wirtualnej wystąpi zdarzenie o identyfikatorze 10103.
Wymagania wstępne systemu Linux	— Za pomocą programu DPM 2012 R2 można wykonywać kopie zapasowe maszyn wirtualnych z systemem Linux. Obsługiwane są tylko migawki zgodne z plikami.
Tworzenie kopii zapasowej maszyn wirtualnych z magazynem CSV	— Na potrzeby magazynu CSV należy zainstalować na serwerze funkcji Hyper-V dostawcę sprzętowego usługi kopiowania woluminów w tle (VSS). W sprawie dostawcy sprzętowego usługi VSS skontaktuj się z dostawcą swojej sieci magazynowania (SAN). — Jeśli jeden węzeł w klastrze CSV zostanie nieoczekiwanie zamknięty, program DPM wykona sprawdzenie spójności, uwzględniając maszyny wirtualne uruchomione w tym węźle. — Jeśli potrzebujesz uruchomić ponownie serwer funkcji Hyper-V z włączoną funkcją szyfrowania dysków BitLocker w klastrze CSV, musisz uruchomić sprawdzenie spójności dla maszyn wirtualnych funkcji Hyper-V.

WYMAGANIE WSTĘPNE	SZCZEGÓŁY
Tworzenie kopii zapasowej maszyn wirtualnych z magazynem SMB	— Aby włączyć ochronę maszyny wirtualnej, włącz funkcję automatycznej instalacji na serwerze z uruchomioną funkcją Hyper-V. — Wyłącz odciążanie przy użyciu technologii TCP Chimney. — Upewnij się, że wszystkie konta machine\$ funkcji Hyper-V mają pełne uprawnienia w określonych udziałach zdalnych plików SMB. — Upewnij się, że ścieżki plików wszystkich składników maszyn wirtualnych podczas odzyskiwania do alternatywnej lokalizacji składają się z maksymalnie 260 znaków. W przeciwnym razie odzyskiwanie może zakończyć się pomyślnie, ale funkcja Hyper-V nie będzie mogła zainstalować maszyny wirtualnej. — Następujące scenariusze nie są obsługiwane: Wdrożenia obejmujące niektóre składniki maszyny wirtualnej znajdujące się na woluminach lokalnych, a pozostałe na woluminach zdalnych; adres IPv4 lub IPv6 serwera plików lokalizacji magazynu; odzyskiwanie maszyny wirtualnej na komputerze używającym zdalnych udziałów SMB. — Musisz włączyć usługę agenta VSS serwera plików na wszystkich serwerach SMB — dodaj ją w obszarze Dodaj role i funkcje > Wybierz role serwera > Usługi plików i magazynowania > Usługi plików > Usługa plików > Usługa agenta VSS serwera plików.

Tworzenie kopii zapasowych maszyn wirtualnych

1. Skonfiguruj [serwer programu DPM](#) i [magazyn](#). Podczas konfigurowania magazynu użyj następujących wytycznych dotyczących pojemności magazynu.
 - Średni rozmiar maszyny wirtualnej — 100 GB
 - Liczba maszyn wirtualnych na serwer programu DPM — 800
 - Całkowity rozmiar 800 maszyn wirtualnych — 80 TB
 - Wymagane miejsce na magazyn kopii zapasowych — 80 TB
2. Skonfiguruj agenta ochrony programu DPM na serwerze funkcji Hyper-V lub na węzłach klastra funkcji Hyper-V. Jeśli wykonujesz kopię zapasową na poziomie gościa, zainstaluj agenta na maszynach wirtualnych, których kopię zapasową na poziomie gościa chcesz utworzyć.
3. W konsoli administratora programu DPM kliknij pozycję **Ochrona > Utwórz grupę ochrony**, aby otworzyć kreatora **Tworzenie nowej grupy ochrony**.
4. Na stronie **Wybierz członków grupy** wybierz maszyny wirtualne, które chcesz chronić za pomocą serwerów hostów funkcji Hyper-V, na których się znajdują. Zalecane jest umieszczenie wszystkich maszyn wirtualnych, które będą miały te same zasady ochrony, w jednej grupie ochrony. W celu efektywnego wykorzystania miejsca włącz wspólną lokalizację. Przekazywanie danych do wspólnej lokalizacji umożliwia umieszczanie danych pochodzących z różnych grup ochrony w tym samym magazynie dyskowym lub taśmowym, tak aby różne źródła danych miały jedną replikę i wolumin punktu odzyskiwania.
5. Na stronie **Wybierz metodę ochrony danych** podaj nazwę grupy ochrony. Wybierz opcję **Chcę uzyskać krótkoterminową ochronę za pomocą dysku** oraz opcję **Chcę uzyskać ochronę online**, aby tworzyć kopie zapasowe danych na platformie Azure za pomocą usługi Azure Backup. Jeśli ta opcja jest niedostępna, dokończ pracę kreatora, aby utworzyć grupę, a następnie zmodyfikuj ustawienia grupy ochrony, aby wybrać tę opcję. Dane można przechowywać na platformie Azure przez maksymalnie 3360 dni.

Jeśli do serwera programu DPM jest podłączona taśma autonomiczna lub biblioteka taśm, można wybrać opcję **Chcę uzyskać długoterminową ochronę za pomocą taśmy**.

6. Na stronie **Określ cele krótkoterminowe > Zakres przechowywania** określ, jak długo mają być przechowywane dane dysku. W obszarze **Częstotliwość synchronizacji** określ, jak często mają być uruchamiane przyrostowe kopie zapasowe danych. Zamiast określać interwał tworzenia przyrostowych kopii zapasowych, możesz włączyć opcję **Bezpośrednio przed punktem odzyskiwania**. Włączenie tego ustawienia spowoduje uruchomienie ekspresowej pełnej kopii zapasowej przez program DPM bezpośrednio przed każdym zaplanowanym punktem odzyskiwania.

- W przypadku ochrony obciążeń aplikacji punkty odzyskiwania są tworzone zgodnie z opcją Częstotliwość synchronizacji, przy założeniu, że aplikacja obsługuje przyrostowe kopie zapasowe. W przeciwnym razie program DPM uruchamia ekspresową pełną kopię zapasową zamiast przyrostowej i tworzy punkty odzyskiwania zgodnie z harmonogramem ekspresowej kopii zapasowej.
- W przypadku włączenia przechowywania długoterminowego na taśmie na stronie **Określ cele długoterminowe > Zakres przechowywania** określ, jak długo mają być przechowywane dane taśmy (1–99 lat). W obszarze Częstotliwość wykonywania kopii zapasowych wybierz odpowiednią częstotliwość wykonywania kopii zapasowych.
- Częstotliwość wykonywania kopii zapasowych zależy od wybranego zakresu przechowywania. Gdy zakres przechowywania wynosi 1–99 lat, można wybrać tworzenie kopii zapasowej codziennie, co tydzień, co dwa tygodnie, co miesiąc, co kwartał, co pół roku lub co rok.
- Gdy zakres przechowywania wynosi 1–11 miesięcy, można wybrać tworzenie kopii zapasowej codziennie, co tydzień, co dwa tygodnie lub co miesiąc. Gdy zakres przechowywania wynosi 1–4 tygodnie, można wybrać tworzenie kopii zapasowej codziennie lub co tydzień.
- W przypadku korzystania z autonomicznej stacji taśm dla pojedynczej grupy ochrony program DPM używa tej samej taśmy do codziennego wykonywania kopii zapasowych do momentu, gdy zabraknie na niej miejsca. Jeśli włączono wspólną lokalizację, zasoby danych będą wspólnie przechowywane na taśmie.
- Jeśli skonfigurowano przechowywanie długoterminowe na taśmie, na stronie **Określanie szczegółów taśmy i biblioteki** określ taśmę i bibliotekę, która będzie używana do tworzenia kopii zapasowych tej grupy ochrony. Można również określić, czy dane kopii zapasowych mają być kompresowane lub szyfrowane.

7. Na stronie **Przejrzyj przydział dysku** przejrzyj miejsce na dysku w puli magazynów przydzielone danej grupie ochrony.

Całkowity rozmiar danych to rozmiar danych, dla których ma zostać utworzona kopia zapasowa, a w obszarze **Miejsce na dysku do udostępnienia w programie DPM** jest widoczna ilość miejsca zalecana przez program DPM dla grupy ochrony. Program DPM wybierze idealną wielkość kopii zapasowej na podstawie ustawień. Opcje wielkości kopii zapasowej można jednak edytować w obszarze **Szczegóły przydziału dysku**. W przypadku obciążeń wybierz z menu rozwijanego preferowany magazyn. Edycja zmienia wartości pozycji **Całkowita ilość miejsca dla magazynu i Wolne miejsce w magazynie** w okienku **Dostępny magazyn dyskowy**. Miejsce poniżej aprowizacji to ilość miejsca, które program DPM sugeruje dodać do woluminu, aby bezproblemowo wykonywać kopie zapasowe w przyszłości.

8. Na stronie **Wybierz metodę tworzenia repliki** określ sposób, w jaki ma zostać wykonana początkowa replikacja danych w grupie ochrony. W przypadku wybrania replikowania za pośrednictwem sieci zaleca się wybranie czasu w godzinach małego obciążenia sieci. W przypadku dużych ilości danych lub nieoptymalnych warunków sieciowych należy wziąć pod uwagę replikację danych w trybie offline za pomocą nośników wymiennych.

9. Na stronie **Opcje sprawdzania spójności** wybierz odpowiedni sposób automatyzacji sprawdzania spójności. Można włączyć uruchamianie sprawdzania tylko wtedy, gdy dane są niespójne, lub zgodnie z harmonogramem. Jeśli nie chcesz konfigurować automatycznego sprawdzania spójności, w dowolnym

momencie możesz uruchomić sprawdzanie ręczne, klikając prawym przyciskiem myszy grupę ochrony i wybierając polecenie **Przeprowadź sprawdzanie spójności**.

Po utworzeniu grupy ochrony następuje replikacja początkowa danych zgodnie z wybraną metodą. Po replikacji początkowej tworzone są poszczególne kopie zapasowe zgodnie z ustawieniami grupy ochrony. Jeśli potrzebujesz odzyskać dane z kopii zapasowej, pamiętaj o następujących kwestiach:

Tworzenie kopii zapasowych maszyn wirtualnych skonfigurowanych do migracji na żywo

Jeśli maszyny wirtualne są związane z migracją na żywo, program DPM nadal będzie je chronić, dopóki agent ochrony programu DPM jest zainstalowany na hoście funkcji Hyper-V. Sposób, w jaki program DPM chroni maszyny wirtualne, zależy od typu odbywającej się migracji na żywo.

Migracja na żywo w ramach klastra — w przypadku migrowania maszyny wirtualnej w ramach klastra program DPM wykrywa ten proces i tworzy kopię zapasową maszyny wirtualnej z nowego węzła klastra bez konieczności żadnej interwencji użytkownika. Ponieważ lokalizacja przechowywania nie została zmieniona, program DPM kontynuuje tworzenie ekspresowych pełnych kopii zapasowych. W ramach skalowanego scenariusza ochrony klastra przy użyciu dwóch serwerów programu DPM maszyna wirtualna chroniona przez serwer 1 programu DPM w dalszym ciągu jest chroniona przez ten serwer niezależnie od lokalizacji, do której jest migrowana.

Migracja na żywo poza klastrem — podczas migracji maszyny wirtualnej między serwerami autonomicznymi, różnymi klastrami lub między serwerem autonomicznym a klastrem program DPM wykrywa ten proces i umożliwia utworzenie kopii zapasowej maszyny wirtualnej bez interwencji użytkownika.

Wymagania dotyczące utrzymania ochrony

Poniżej przedstawiono wymagania dotyczące utrzymania ochrony podczas migracji na żywo:

- Hosty funkcji Hyper-V dla maszyn wirtualnych muszą znajdować się w chmurze programu System Center VMM na serwerze VMM, na którym działa co najmniej program System Center 2012 z dodatkiem SP1.
- Agent ochrony programu DPM musi być zainstalowany na wszystkich hostach funkcji Hyper-V.
- Serwery programu DPM muszą być podłączone do serwera VMM. Wszystkie serwery hosta funkcji Hyper-V w chmurze programu VMM również muszą być podłączone do serwerów programu DPM. Dzięki temu program DPM może komunikować się z serwerem programu VMM, aby program DPM mógł dowiedzieć się, na którym serwerze hosta funkcji Hyper-V maszyna wirtualna jest aktualnie uruchomiona, i utworzyć nową kopię zapasową z tego serwera funkcji Hyper-V. Jeśli połączenie z serwerem funkcji Hyper-V nie może zostać ustanowione, tworzenie kopii zapasowej zakończy się niepowodzeniem i wyświetleniem komunikatu informującego, że agent ochrony programu DPM jest nieosiągalny.
- Wszystkie serwery programu DPM, serwery VMM i serwery hosta funkcji Hyper-V muszą być w tej samej domenie.

Szczegółowe informacje o migracji na żywo

W przypadku tworzenia kopii zapasowej podczas migracji na żywo należy pamiętać o następujących kwestiach:

- Ochrona migracji na żywo nie obsługuje wykonywania kopii zapasowej na taśmie.
- Jeśli magazyn jest transferowany w procesie migracji na żywo, program DPM przeprowadza pełne sprawdzanie spójności maszyny wirtualnej, a następnie kontynuuje tworzenie ekspresowych pełnych kopii zapasowych. Gdy odbywa się migracja magazynu na żywo, funkcja Hyper-V reorganizuje wirtualny dysk twardy (VHD) lub dysk VHDX, co powoduje jednorazowy gwałtowny wzrost rozmiaru danych kopii zapasowej programu DPM.
- Na hoście maszyny wirtualnej włącz funkcję automatycznego instalowania, aby umożliwić ochronę wirtualną, i wyłącz odciążanie przy użyciu technologii TCP Chimney.

- Program DPM używa portu 6070 jako portu domyślnego w celu hostowania usługi pomocnika DPM-VMM. Aby zmienić rejestr:

1. Przejdź do klucza **HKLM\Software\Microsoft\Microsoft Data Protection Manager\Configuration**.
2. Utwórz 32-bitową wartość DWORD: DpmVmmHelperServicePort i zapisz zaktualizowany numer portu jako część klucza rejestru.
3. Otwórz plik

```
<Install directory>\Microsoft System Center  
2012\DPM\DPM\VmmHelperService\VmmHelperServiceHost.exe.config
```

i zmień numer portu z 6070 na nowy port. Na przykład:

```
<add baseAddress="net.tcp://localhost:6080/VmmHelperService/" />
```

4. Uruchom ponownie usługę pomocnika DPM-VMM, a następnie uruchom ponownie usługę programu DPM.

Konfiguracja ochrony migracji na żywo

Aby skonfigurować ochronę migracji na żywo:

1. Skonfiguruj serwer programu DPM i jego magazyn, a następnie zainstaluj agenta ochrony programu DPM na każdym serwerze hosta funkcji Hyper-V lub w węźle klastra w chmurze programu VMM. Jeśli używasz magazynu SMB w klastrze, zainstaluj agenta ochrony programu DPM na wszystkich węzłach klastra.
2. Zainstaluj konsolę programu VMM jako składnik klienta na serwerze programu DPM, tak aby program DPM mógł komunikować się z serwerem VMM. Konsola powinna mieć taką samą wersję, jaka działa na serwerze programu VMM.
3. Przypisz konto DPMMachineName\$ na serwerze zarządzania programem VMM jako konto administratora przeznaczone tylko do odczytu.
4. Połącz wszystkie serwery hostów funkcji Hyper-V ze wszystkimi serwerami programu DPM za pomocą polecenia cmdlet `Set-DPMGlobalProperty` programu PowerShell. Polecenie cmdlet przyjmuje wiele nazw serwerów programu DPM. Użyj formatu:

```
Set-DPMGlobalProperty -dpmservername <dpmservername> -knownvmmserver <vmmservername>
```

 Aby uzyskać więcej informacji, zobacz [Set-DPMGlobalProperty](#).
5. Po odnalezieniu w programie VMM wszystkich maszyn wirtualnych uruchomionych na hostach funkcji Hyper-V w chmurach programu VMM skonfiguruj grupę ochrony i dodaj maszyny wirtualne, które chcesz chronić. Zwróć uwagę, że w przypadku scenariuszy z mobilnością maszyny wirtualnej w celu ochrony powinny być włączone automatyczne sprawdzenia spójności na poziomie grupy ochrony.
6. Po skonfigurowaniu ustawień, gdy maszyna wirtualna jest migrowana z jednego klastra do innego, tworzenie wszystkich kopii zapasowych jest kontynuowane zgodnie z oczekiwaniami. Możesz sprawdzić, czy migracja na żywo jest włączona zgodnie z oczekiwaniami, w następujący sposób:

- a. Sprawdź, czy usługa pomocnika DPM-VMM jest uruchomiona. Jeśli nie, uruchom ją.
- b. Otwórz program Microsoft SQL Server Management Studio i połącz się z wystąpieniem, które hostuje bazę danych programu DPM (DPMDB). W bazie danych DPMDB uruchom następujące zapytanie:

```
SELECT TOP 1000 [PropertyName] , [PropertyValue] FROM [DPMDB].[dbo].[tbl_DLS_GlobalSetting] .
```

To zapytanie zawiera właściwość o nazwie `KnownVMMServer`. Ta wartość powinna być taka sama jak wartość dostarczona z poleceniem cmdlet `Set-DPMGlobalProperty`.

- c. Uruchom następujące zapytanie, aby zweryfikować parametr `VMMIdentifier` w lokalizacji `PhysicalPathXML` dla konkretnej maszyny wirtualnej. Zastąp `VMName` nazwą maszyny wirtualnej.

```
select cast(PhysicalPath as XML) from tbl_IM_ProtectedObject where DataSourceId in (select  
datasourceid from tbl_IM_DataSource where DataSourceName like '%<VMName>%')
```

- d. Otwórz plik .xml, który zwraca to zapytanie, i sprawdź, czy w polu *VMMIdentifier* znajduje się wartość.

Uruchamianie ręcznej migracji

Po wykonaniu czynności opisanych w poprzednich sekcjach i ukończeniu zadania Menedżera podsumowania programu DPM następuje włączenie migracji. Domyślnie to zadanie jest uruchamiane o północy i wykonywane każdego ranka. Jeśli chcesz uruchomić ręczną migrację w celu sprawdzenia, czy wszystko działa zgodnie z oczekiwaniami, wykonaj następujące czynności:

1. Otwórz program SQL Server Management Studio i połącz się z wystąpieniem, które hostuje bazę danych programu DPM.

2. Uruchom następujące zapytanie:

```
select * from tbl_SCH_ScheduleDefinition where JobDefinitionID='9B30D213-B836-4B9E-97C2-DB03C3EB39D7'.
```

To zapytanie zwraca identyfikator harmonogramu **ScheduleID**. Zapisz ten identyfikator, ponieważ użyjesz go w następnym kroku.

3. W programie SQL Server Management Studio rozwiń pozycję **Agent programu SQL Server**, a następnie rozwiń pozycję **Zadania**. Kliknij prawym przyciskiem myszy zapisany identyfikator **ScheduleID** i wybierz polecenie **Uruchom zadanie w kroku**.

Należy pamiętać, że na wydajność tworzenia kopii zapasowej ma wpływ wykonywanie zadania. Czas potrzebny na zakończenie zadania zależy od rozmiaru i skali wdrożenia.

Tworzenie kopii zapasowych maszyn wirtualnych repliki

Jeśli program DPM jest uruchomiony w systemie Windows Server 2012 R2 lub nowszym, możesz wykonać kopie zapasowe maszyn wirtualnych replik na serwerze pomocniczym. Jest to przydatne z kilku powodów:

Ogranicza wpływ tworzenia kopii zapasowej na obciążenie pracą — wykonywanie kopii zapasowej maszyny wirtualnej powoduje pewne nadmiarowe obciążenie podczas tworzenia migawki. Dzięki przeniesieniu procesu tworzenia kopii zapasowej do zdalnej lokalizacji pomocniczej operacja wykonywania kopii zapasowej nie wpływa już na obciążenie pracą. Ma to zastosowanie tylko do wdrożeń, w których kopia zapasowa jest przechowywana w lokalizacji zdalnej. Na przykład możesz korzystać z codziennych kopii zapasowych i przechowywać dane lokalnie w celu zapewnienia szybkiego przywracania, ale co miesiąc lub co kwartał tworzyć kopie zapasowe z maszyn wirtualnych replik przechowywanych zdalnie w celu przechowywania długoterminowego.

Oszczędza przepustowość — w typowych wdrożeniach w zdalnym oddziale lub siedzibie firmy potrzebne jest zapewnienie odpowiedniej przepustowości do transferu danych kopii zapasowych między lokalizacjami. Jeśli stworzysz strategię replikacji i pracy awaryjnej, oprócz opracowania strategii wykonywania kopii zapasowej danych możesz zmniejszyć ilość nadmiarowych danych przesyłanych w sieci. Wykonywanie kopii zapasowych danych maszyny wirtualnej repliki zamiast podstawowej pozwoli zmniejszyć nakłady związane z wysyłaniem danych kopii zapasowej w sieci.

Umożliwia wykonywanie kopii zapasowych dostawcy usług hostingowych — hostowanego centrum danych można użyć jako lokalizacji repliki, co powoduje, że pomocnicze centrum danych nie jest potrzebne. W takim przypadku umowa SLA z dostawcą usług hostingowych wymaga spójnych kopii zapasowych maszyn wirtualnych replik.

Maszyna wirtualna repliki jest wyłączona do momentu zainicjowania trybu failover, a usługa VSS nie może zagwarantować kopii zapasowej maszyny wirtualnej repliki spójnej na poziomie aplikacji. W związku z tym kopia zapasowa repliki maszyny wirtualnej będzie tylko spójna na poziomie awarii. Jeśli nie można zagwarantować spójności na poziomie awarii, tworzenie kopii zapasowej zakończy się niepowodzeniem, a taka sytuacja może wystąpić w kilku przypadkach:

- Maszyna wirtualna repliki nie jest w dobrej kondycji i jest w stanie krytycznym.
- Maszyna wirtualna repliki jest ponownie synchronizowana (w stanie ponownej synchronizacji w toku lub w

stanie konieczności wykonania ponownej synchronizacji).

- Początkowa replikacja maszyny wirtualnej między lokalizacją główną a pomocniczą jest w toku lub jest oczekiwana.
- Dzienniki .hrl są stosowane do maszyny wirtualnej repliki lub poprzednia czynność zastosowania dzienników .hrl na dysku wirtualnym nie powiodła się, została anulowana lub przerwana.
- Trwa migracja lub praca w trybie failover maszyny wirtualnej repliki

Odzyskiwanie kopii zapasowych maszyn wirtualnych

Gdy możesz odzyskać kopię zapasową maszyny wirtualnej, użyj Kreatora odzyskiwania, aby wybrać maszynę wirtualną i określony punkt odzyskiwania. Aby otworzyć Kreatora odzyskiwania i odzyskać maszynę wirtualną:

1. W konsoli administratora programu DPM wpisz nazwę maszyny wirtualnej lub rozwiń listę elementów chronionych i wybierz maszynę wirtualną, którą chcesz odzyskać.
2. W okienku **Punkty odzyskiwania dla** kliknij w kalendarzu dowolną datę, aby wyświetlić dostępne punkty odzyskiwania. Następnie w okienku **Ścieżka** wybierz punkt odzyskiwania, którego chcesz użyć w Kreatorze odzyskiwania.
3. W menu **Akcje** kliknij pozycję **Odzyskaj**, aby otworzyć Kreatora odzyskiwania.

Wybrana maszyna wirtualna i punkt odzyskiwania są wyświetlane na ekranie **Przegląd wybranego elementu do odzyskania**. Kliknij przycisk **Next** (Dalej).

4. Na ekranie **Wybieranie typu odzyskiwania** wybierz, dokąd chcesz przywrócić dane, a następnie kliknij przycisk **Dalej**.

- **Odzyskiwanie do oryginalnego wystąpienia:** podczas odzyskiwania do oryginalnego wystąpienia oryginalny dysk VHD jest usuwany. Program DPM odzyskuje dysk VHD i inne pliki konfiguracji do lokalizacji oryginalnej za pomocą składnika zapisywania usługi VSS funkcji Hyper-V. Po zakończeniu procesu odzyskiwania maszyny wirtualne nadal zapewniają dużą dostępność. Aby odzyskiwanie mogło się odbyć, musi być dostępna grupa zasobów. Jeśli grupa nie jest dostępna, wykonaj odzyskiwanie do lokalizacji alternatywnej, a następnie przełącz maszynę wirtualną w tryb wysokiej dostępności.

- **Odzyskiwanie do dowolnego hosta jako maszyna wirtualna:** program DPM obsługuje odzyskiwanie do lokalizacji alternatywnej (ALR), które zapewnia bezproblemowe odzyskiwanie chronionej maszyny wirtualnej funkcji Hyper-V do innego hosta funkcji Hyper-V, niezależnie od architektury procesora. Maszyny wirtualne funkcji Hyper-V, które są odzyskiwane do węzła klastra, nie będą mieć wysokiej dostępności. Jeśli wybierzesz tę opcję, Kreator odzyskiwania wyświetli dodatkowy ekran w celu identyfikacji miejsca docelowego i ścieżki docelowej.

- **Kopiowanie do folderu sieciowego:** program DPM obsługuje odzyskiwanie na poziomie elementu (ILR), które pozwala na poziomie elementu odzyskiwać pliki, foldery, woluminy i wirtualne dyski twarde (VHD) z kopii zapasowych na poziomie hosta maszyn wirtualnych funkcji Hyper-V do udziału sieciowego lub woluminu na serwerze chronionym przez program DPM. Do przeprowadzenia odzyskiwania na poziomie elementu nie jest wymagane, aby w systemie gościa był zainstalowany agent ochrony programu DPM. Jeśli wybierzesz tę opcję, Kreator odzyskiwania wyświetli dodatkowy ekran w celu identyfikacji miejsca docelowego i ścieżki docelowej.

5. W obszarze **Określanie opcji odzyskiwania** skonfiguruj opcje odzyskiwania i kliknij przycisk **Dalej**:

- Jeśli odzyskujesz maszynę wirtualną w warunkach niskiej przepustowości, kliknij pozycję **Modyfikuj**, aby włączyć pozycję **Ograniczenie przepustowości sieci**. Po włączeniu opcji ograniczania przepustowości możesz określić przepustowość, którą chcesz udostępnić, i czas, kiedy ta przepustowość jest dostępna.

- Jeśli sieć jest skonfigurowana, wybierz pozycję **Włącz odzyskiwanie na podstawie sieci SAN z użyciem migawek sprzętowych**.
 - Wybierz pozycję **Wyślij wiadomość e-mail po zakończeniu odzyskiwania**, a następnie wprowadź adresy e-mail, jeśli chcesz, aby powiadomienia e-mail były wysyłane po zakończeniu procesu odzyskiwania.
6. Na ekranie Podsumowanie upewnij się, że wszystkie szczegóły są poprawne. Jeśli szczegóły nie są poprawne lub chcesz wprowadzić zmiany, kliknij przycisk **Wstecz**. Jeśli ustawienia są poprawne, kliknij przycisk **Odzyskaj**, aby rozpocząć proces odzyskiwania.
7. Ekran **Stan odzyskiwania** zawiera informacje o zadaniu odzyskiwania.

Tworzenie kopii zapasowej programu Exchange przy użyciu programu DPM

11.12.2019 • 70 minutes to read

Program System Center Data Protection Manager (DPM) umożliwia tworzenie kopii zapasowych i odzyskiwanie dla programów Exchange 2013 i Exchange 2016. Aby zapewnić ochronę całego wdrożenia programu Exchange, należy skonfigurować ochronę woluminów, stanu systemu lub odzyskiwania pełnego systemu operacyjnego. Ten artykuł zawiera instrukcje dotyczące konfigurowania programu DPM, aby można było chronić wdrożenie programu Exchange. Jeśli masz duże wdrożenie programu Exchange, Użyj grupy dostępności bazy danych (DAG) do skalowania ochrony baz danych skrzynek pocztowych programu Exchange. Aby w pełni chronić wdrożenie programu Exchange, oprócz tworzenia kopii zapasowych baz danych poczty należy utworzyć kopie zapasowe ról programu Exchange Server, takich jak serwer dostępu klienta lub usługa transportu na serwerach skrzynek pocztowych.

Wymagania wstępne i ograniczenia

Przed wdrożeniem programu DPM w celu ochrony programów Exchange 2013 i Exchange 2016 Sprawdź wymagania wstępne dotyczące wdrażania:

- Przejrzyj [Informacje o wersji programu DPM](#)
- Zapoznaj się z artykułem, [co jest obsługiwane i co nie dotyczy programu DPM?](#), w przypadku jakichkolwiek problemów z programem Exchange.
- Upewnij się, że zarówno na serwerze programu Exchange, jak i na serwerze programu DPM zostały zainstalowane te same wersje plików Eseutil.exe i Ese.dll. Na przykład jeśli korzystasz z 64-bitowej wersji programu DPM, musisz mieć 64-bitowe wersje plików eseutil.exe i ese.dll. W przypadku aktualizacji tych plików na serwerze Exchange należy również zaktualizować pliki na serwerze programu DPM. Pliki `.ese` i `.eseutil` znajdują się zwykle w lokalizacji, `C:\Program Files\Microsoft\Exchange Server\V15\Bin`.

Aby zachować aktualne kopie:

1. W wierszu polecenia przejdź do katalogu `<DPM installation folder>\Bin`.
2. Wpisz polecenie fsutil w następujący sposób, aby utworzyć twardy link do pliku Eseutil.exe:

```
fsutil hardlink create <link> <target>
```

Na przykład w typowym typie instalacji:

```
fsutil hardlink create "c:\program files\microsoft\dpm\bin\eseutil.exe" "c:\program files\microsoft\Exchange\bin\eseutil.exe"
```

- Zainstaluj [pakiet Visual C++ Redistributable dla programu Visual Studio 2012 Update](#).
- Aby chronić węzeł grupy dostępności bazy danych (DAG) programu Exchange 2013 i programu Exchange 2016, Zainstaluj agenta ochrony programu DPM na węźle. Należy pamiętać, że można chronić różne węzły DAG z różnych serwerów DPM. Tylko jeden węzeł może być chroniony za pomocą tylko jednego serwera DPM.
- Program DPM 2012 (i nowsze) ma limit rozmiaru puli magazynu równy 120 terabajt (TB). Istnieje limit 80 TB dla woluminów repliki programu DPM i limit 40 TB dla woluminów punktów odzyskiwania. W przypadku ochrony dużego wdrożenia programu Exchange należy znać limit rozmiaru skrzynki pocztowej użytkownika oraz liczbę użytkowników lub skrzynek pocztowych. Liczba użytkowników lub skrzynek

pocztowych określa maksymalny rozmiar skrzynki pocztowej. Jeśli skrzynki pocztowe pozostają w granicach, Liczba skrzynek pocztowych określa liczbę baz danych programu Exchange, które mogą być chronione przez jeden program DPM. Użyj liczby użytkowników przypisanych do bazy danych i ich limitów skrzynek pocztowych, aby obliczyć maksymalny rozmiar możliwy dla każdej bazy danych programu Exchange. Na przykład jeśli maksymalny rozmiar skrzynki pocztowej użytkownika 8 GB, jeden serwer DPM może chronić do 10 000 skrzynek pocztowych. Jeśli maksymalny rozmiar skrzynki pocztowej użytkownika jest większy niż 8 GB lub w przypadku, gdy więcej niż 10 000 skrzynek pocztowych użytkowników wymaga ochrony, skonfiguruj serwer programu Exchange z DAG. Aby zapewnić pełną ochronę, użyj dodatkowych serwerów programu DPM. Węzeł programu Exchange może być chroniony tylko przez jeden serwer DPM. W związku z tym liczba węzłów programu Exchange powinna być równa lub większa niż liczba serwerów programu DPM wymaganych do ochrony wszystkich baz danych programu Exchange.

- Program DPM działa z dowolną rolą bazy danych. Program DPM można skonfigurować tak, aby chronił serwer hostujący kolekcję aktywnych lub pasywnych baz danych skrzynek pocztowych.
- Skonfiguruj jedną pełną kopię zapasową dziennie i częstotliwość synchronizacji zgodnie z wymaganiami dotyczącymi obciążenia dzienników programu Exchange. W przypadku ochrony więcej niż jednej kopii bazy danych skrzynek pocztowych programu Exchange (na przykład podczas ochrony członków DAG) skonfiguruj jeden węzeł dla pełnych kopii zapasowych i pozostały do kopiowania kopii zapasowych. Kopie kopii zapasowych nie powodują obcinania plików dziennika.
- Chronić co najmniej dwie kopie każdej bazy danych skrzynek pocztowych. Do przechowywania można używać niedrogich dysków Serial Advanced Technology (SATA) lub kilku dysków JBOD.
- Dla synchronizacji skrzynki pocztowej ustaw częstotliwość minimalną na więcej niż 15 minut. Rozpocznij od konfiguracji aktualnych zasad tworzenia kopii zapasowych, a następnie stopniowo zwiększaj liczbę punktów odzyskiwania. Wykonywanie jednego lub dwóch zadań tworzenia ekspresowych pełnych kopii zapasowych dziennie, przy częstotliwości synchronizacji wynoszącej dwie godziny, to rozsądne rozwiązanie. Aby uzyskać optymalną częstotliwość synchronizacji, należy wziąć pod uwagę ilość danych, wpływ na wydajność oraz ilość wymaganą do przechowywania replik.
- Program Exchange 2013 i program Exchange 2016 mogą obsługiwać maksymalnie osiem równoległych kopii zapasowych. Aby obsłużyć zadania tworzenia równoległych kopii zapasowych bazy danych programu Exchange dla serwera Exchange, utwórz wiele grup ochrony (maksymalnie osiem) i dodaj bazy danych programu Exchange do każdej grupy ochrony.
- Zachowując dane programu Exchange, należy pamiętać o następujących kwestiach:
 - **Dodawanie baz danych skrzynek pocztowych do serwera.** W przypadku tworzenia lub dodawania nowych baz danych skrzynek pocztowych do chronionej grupy magazynów na serwerze Exchange te bazy danych są automatycznie dodawane do zadań replikacji i ochrony w programie DPM. Można dodać bazy danych skrzynki pocztowej w trakcie tworzenia przyrostowych kopii zapasowych dopiero po zakończeniu tworzenia pełnych kopii zapasowych.
 - **Zmiana ścieżek plików bazy danych skrzynek pocztowych.** Jeśli chroniona baza danych lub pliki dziennika zostaną przeniesione do woluminu zawierającego dane chronione za pomocą programu DPM, ochrona będzie kontynuowana. W przypadku przeniesienia chronionej bazy danych lub plików dziennika do woluminu, który nie jest chroniony za pomocą programu DPM, zostanie wyświetlony alert i zadania ochrony zakończą się niepowodzeniem. Aby rozwiązać alert, kliknij link **Modyfikuj zadanie ochrony** w obszarze szczegółów alertu, po czym uruchom sprawdzanie spójności.
 - **Odinstalowywanie baz danych skrzynek pocztowych.** W przypadku odinstalowywania chronionej bazy danych skrzynki pocztowej zadanie ochrony dla tej określonej bazy danych kończy się niepowodzeniem. Replika zostaje oznaczona jako niespójna, gdy program DPM uruchamia kolejne zadanie tworzenia ekspresowej pełnej kopii zapasowej.

- **Zmiana nazw baz danych skrzynek pocztowych.** Jeśli musisz zmienić nazwę bazy danych skrzynki pocztowej, wyłącz ochronę i włącz ochronę bazy danych ponownie. Przed ponownym włączeniem ochrony bazy danych tworzenie kopii zapasowych jest kontynuowane, ale wyliczanie skrzynki pocztowej kończy się niepowodzeniem.

Dlaczego warto wykonywać kopie zapasowe programu Exchange przy użyciu programu DPM?

Podczas podejmowania decyzji o utworzeniu kopii zapasowej danych programu Exchange przy użyciu programu Exchange 2013 i programu Exchange 2016 Native Data Protection lub DPM należy wziąć pod uwagę następujące kwestie:

Ochrona danych natywnych umożliwia:

- Odzyskiwanie po awarii
- Odzyskiwanie przypadkowo usuniętych elementów
- Przechowuje dane przez dłuższy okres.
- Tworzenie migawek baz danych z określonego momentu

Ochrona danych natywnych może być mimo tego niewystarczająca, jeśli występują błędy aplikacji, uszkodzenia lub zdarzenia związane z zabezpieczeniami i złośliwym oprogramowaniem. W takich sytuacjach program DPM oferuje następujące korzyści:

- Mniejsza liczba wymaganych grup DAG — ochrona danych natywnych wymaga dodatkowych serwerów skrzynek pocztowych do hostowania kopii aktywnych danych. Tworzenie kopii zapasowych przy użyciu funkcji ochrony programu DPM w żaden sposób nie zależy od grup DAG.
- Prostsze przywracanie — program DPM udostępnia proste i scentralizowane odzyskiwanie danych z kopii zapasowych z określonego punktu w czasie.
- Dłuższy zakres przechowywania — program DPM oferuje dłuższe czasy przechowywania kopii zapasowych danych. Ochrona danych natywnych jest ograniczona do 14 dni.
- Spójne tworzenie kopii zapasowych obciążeń dotyczących rozwiązań firmy Microsoft — program DPM oferuje scentralizowany i prosty proces tworzenia kopii zapasowych danych i ich odzyskiwania dla obciążeń dotyczących rozwiązań firmy Microsoft, w tym programu Exchange, serwerów plików, programu SQL Server, funkcji Hyper-V i programu SharePoint.

Przed rozpoczęciem

1. **Wdrażanie programu DPM** — sprawdź, czy program DPM został poprawnie zainstalowany i wdrożony. Jeśli nie zostało to jeszcze zrobione, zobacz:
 - Wymagania systemowe dotyczące programu DPM
 - [Co program DPM może umieścić w kopii zapasowej?](#)
 - [Elementy obsługiwane i nieobsługiwane przez program DPM](#)
 - [Instalowanie programu DPM](#)
2. Konfigurowanie magazynu — dane kopii zapasowej można przechowywać na dysku, na taśmie i w chmurze przy użyciu platformy Azure. Więcej informacji znajduje się w temacie [Prepare data storage](#) (Przygotowanie magazynu danych).
3. **Skonfiguruj agenta ochrony DPM** — Agent musi być zainstalowany na serwerze Exchange. Zapoznaj się

Konfigurowanie kopii zapasowej

1. Kliknij pozycję **ochrona > Akcje > Utwórz grupę ochrony**, aby otworzyć kreatora **tworzenia nowej grupy ochrony** w konsoli programu DPM.
2. Na stronie **Wybierz typ grupy ochrony** wybierz pozycję **Serwery**.
3. Na stronie **Wybierz członków grupy** wybierz wszystkie grupy DAG zawierające dane, które chcesz chronić. Dla każdego serwera programu Exchange można również wybrać opcję tworzenia kopii zapasowej stanu systemu lub pełnej kopii zapasowej kompletnego stanu systemu (zawierającej dane o stanie systemu). Jest to przydatne, jeśli chcesz mieć możliwość odzyskania całego serwera, a nie tylko danych. [Wdrażanie grup ochrony](#).
4. W obszarze **Wybierz metodę ochrony danych** określ, jak mają być obsługiwane krótkoterminowe i długoterminowe kopie zapasowe. Krótkoterminowa kopia zapasowa jest zawsze najpierw tworzona na dysku z opcją przeniesienia kopii zapasowej z dysku do chmury platformy Azure za pomocą usługi Azure Backup (na potrzeby przechowywania krótkoterminowego lub długoterminowego). Zamiast długoterminowej kopii zapasowej w chmurze możesz również skonfigurować długoterminową kopię zapasową na autonomicznym urządzeniu taśmowym lub w bibliotece taśm połączonej z serwerem programu DPM.
5. Na stronie **Określ opcje ochrony programu Exchange** wybierz pozycję **Uruchom program Eseutil**, aby sprawdzić integralność danych w celu sprawdzenia integralności baz danych programu Exchange. Spowoduje to przeniesienie operacji sprawdzania spójności kopii zapasowej z programu Exchange Server na serwer programu DPM, co oznacza, że wpływ operacji we/wy programu Eseutil.exe na program Exchange Server podczas tworzenia kopii zapasowej zostanie wyeliminowany. Aby chronić grupę DAG, upewnij się, że wybierasz opcję Uruchom tylko dla plików dziennika (zalecane dla serwerów DAG). Jeśli plik eseutil nie został wcześniej skopiowany, wystąpi błąd.
6. Na stronie **Określ ochronę Exchange DAG** wybierz bazy danych, które chcesz skopiować w postaci pełnej kopii zapasowej lub kopii kopii zapasowej, korzystając z list **Kopie bazy danych wybrane do pełnej kopii zapasowej** lub **Kopie bazy danych wybrane do kopii zapasowej**. W celu ochrony wielu kopii tej samej bazy danych można wybrać tylko jedną kopię dla pełnej kopii zapasowej, a następnie wybrać pozostałe kopie jako kopie kopii zapasowej.
7. W polu **Wybierz cele krótkoterminowe** określ sposób tworzenia kopii zapasowej w krótkoterminowym magazynie na dysku. W obszarze **Zakres przechowywania** określ, jak długo chcesz przechowywać dane na dysku. W obszarze **Częstotliwość synchronizacji** określ, jak często chcesz zapisywać przyrostowe kopie zapasowe na dysku. Jeśli nie chcesz ustawiać interwału kopii zapasowych, możesz sprawdzić tuż przed punktem odzyskiwania, aby program DPM wykonał ekspresową pełną kopię zapasową tuż przed zaplanowaniem każdego punktu odzyskiwania.
8. Jeśli chcesz utworzyć długoterminową kopię zapasową danych na taśmie, na stronie **Określ cele długoterminowe** wskaż, jak długo chcesz przechowywać dane na taśmie (od 1 roku do 99 lat). W obszarze **Częstotliwość wykonywania kopii zapasowych** określ, jak często mają być wykonywane kopie zapasowe na taśmie. Częstotliwość zależy od wybranego zakresu przechowywania:
 - Gdy zakres przechowywania wynosi 1–99 lat, można wybrać tworzenie kopii zapasowej codziennie, co tydzień, co dwa tygodnie, co miesiąc, co kwartał, co pół roku lub co rok.
 - Gdy zakres przechowywania wynosi 1–11 miesięcy, można wybrać tworzenie kopii zapasowej codziennie, co tydzień, co dwa tygodnie lub co miesiąc.
 - Gdy zakres przechowywania wynosi 1–4 tygodnie, można wybrać tworzenie kopii zapasowej codziennie lub co tydzień.

W przypadku korzystania z autonomicznej stacji taśm dla pojedynczej grupy ochrony program DPM używa tej samej taśmy do codziennego wykonywania kopii zapasowych do momentu, gdy zabraknie na niej miejsca. Na taśmie można również zapisywać dane z różnych grup ochrony.

Na stronie **Określanie szczegółów taśmy i biblioteki** określ taśmę lub bibliotekę, która ma być używana, oraz czy dane na taśmie mają być kompresowane i szyfrowane.

9. Na stronie **Przejrzyj przydział dysku** przejrzyj miejsce na dysku w puli magazynów przydzielone danej grupie ochrony.

Całkowity rozmiar danych to rozmiar danych, dla których ma zostać utworzona kopia zapasowa, a w obszarze **Miejsce na dysku do udostępnienia w programie DPM** jest widoczna ilość miejsca zalecana przez program DPM dla grupy ochrony. Program DPM wybierze idealną wielkość kopii zapasowej na podstawie ustawień. Opcje wielkości kopii zapasowej można jednak edytować w obszarze **Szczegóły przydziału dysku**. W przypadku obciążeń wybierz z menu rozwijanego preferowany magazyn. Edycja zmienia wartości pozycji **Całkowita ilość miejsca dla magazynu i Wolne miejsce w magazynie** w okienku **Dostępny magazyn dyskowy**. Miejsce poniżej apro wizacji to ilość miejsca, które program DPM sugeruje dodać do woluminu, aby bezproblemowo wykonywać kopie zapasowe w przyszłości.

10. W polu **Wybierz metodę tworzenia repliki** określ, jak chcesz obsługiwać początkową pełną replikację danych. W przypadku wybrania replikowania za pośrednictwem sieci zaleca się wybranie czasu w godzinach małego obciążenia sieci. W przypadku dużych ilości danych lub nieoptymalnych warunków sieciowych należy wziąć pod uwagę replikację danych w trybie offline za pomocą nośników wymiennych.
11. W polu **Wybierz opcje sprawdzania spójności** wybierz sposób automatyzacji sprawdzania spójności. Można włączyć uruchamianie sprawdzania tylko wtedy, gdy dane są niespójne, lub zgodnie z harmonogramem. Jeśli nie chcesz konfigurować automatycznego sprawdzania spójności, w dowolnym momencie możesz uruchomić sprawdzanie ręczne, klikając prawym przyciskiem myszy grupę ochrony w obszarze **Ochrona** w konsoli programu DPM i wybierając polecenie **Przeprowadź sprawdzanie spójności**.
12. Jeśli wybrano opcję tworzenia kopii zapasowych w chmurze przy użyciu usługi Azure Backup, sprawdź, czy na stronie **Określanie danych chronionych w trybie online** zaznaczono obciążenia, dla których ma być tworzona kopia zapasowa na platformie Azure.
13. W obszarze **Określanie harmonogramu tworzenia kopii zapasowych online** określ, jak często mają być wykonywane przyrostowe kopie zapasowe na platformie Azure. Wykonywanie kopii zapasowych można zaplanować na każdy dzień/tydzień/miesiąc/rok, natomiast godziny/daty pozwalają ustalić konkretny czas uruchomienia wykonywania kopii zapasowych. Kopie zapasowe mogą być tworzone maksymalnie dwa razy dziennie. Zawsze podczas wykonywania kopii zapasowej na platformie Azure jest tworzony punkt odzyskiwania danych na podstawie kopii danych przechowywanych w kopii zapasowej na dysku programu DPM.
14. W polu **Określ zasady przechowywania danych online** możesz określić sposób przechowywania na platformie Azure punktów odzyskiwania tworzonych na podstawie kopii zapasowych wykonywanych co dzień/tydzień/miesiąc/rok.
15. W polu **Wybierz replikację online** określ, jak będzie wykonywana początkowa pełna replikacja danych. Możesz wykonywać replikację za pośrednictwem sieci lub tworzyć kopie zapasowe offline (rozmieszczanie offline). W przypadku kopii zapasowych offline używana jest funkcja Azure Import. [Przeczytaj więcej](#).
16. Na stronie **Podsumowanie** przejrzyj ustawienia. Po kliknięciu pozycji **Utwórz grupę** następuje początkowa replikacja danych. Po ukończeniu replikacji grupa ochrony będzie mieć stan **OK** na stronie **Stan**. Następnie odbywa się tworzenie kopii zapasowych zgodnie z ustawieniami grupy ochrony.

Monitorowanie

Po utworzeniu grupy ochrony następuje replikacja początkowa i program DPM rozpoczyna wykonywanie kopii zapasowej i synchronizowanie danych programu Exchange. Program DPM monitoruje synchronizację początkową i tworzenie kolejnych kopii zapasowych. Możesz monitorować dane programu Exchange na kilka sposobów:

- Za pomocą domyślnej funkcji monitorowania programu DPM można skonfigurować powiadomienia na potrzeby aktywnego monitorowania (przez publikowanie alertów i konfigurowanie powiadomień). Powiadomienia mogą być przysyłane pocztą e-mail w przypadku alertów krytycznych, ostrzeżeń lub informacji oraz w przypadku informacji o stanie wystąpień procesu odzyskiwania.
- Korzystając z programu Operations Manager, można publikować alerty z poziomu centralnej lokalizacji.

Konfigurowanie powiadomień dotyczących monitorowania

1. W Konsola administratora programu DPM kliknij pozycję **monitorowanie** > **akcji** > **Opcje**.
2. Kliknij pozycję **Serwer SMTP**, a następnie wpisz nazwę serwera, port i adres e-mail, z którego będą wysyłane powiadomienia. Adres musi być prawidłowy.
3. W obszarze **uwierzytelniony serwer SMTP** wpisz nazwę użytkownika i hasło. Nazwa użytkownika i hasło muszą odpowiadać nazwie konta domeny należącego do osoby, której adres „Od” został opisany w poprzednim kroku. W przeciwnym razie dostarczanie powiadomień nie powiedzie się.
4. Aby przetestować ustawienia serwera SMTP, kliknij pozycję **Wyślij testową wiadomość e-mail**, wpisz adres e-mail, na który serwer programu DPM ma przesłać wiadomość testową, a następnie kliknij przycisk **OK**. Kliknij kolejno pozycje **Opcje** > **Powiadomienia**, a następnie wybierz typy alertów, o których odbiorcy chcą być powiadamiani. W polu **Odbiorcy** wpisz adres e-mail każdego odbiorcy, do którego program DPM ma przysyłać kopie powiadomień.
5. Aby przetestować ustawienia serwera SMTP, kliknij pozycję **Wyślij testowe powiadomienie e-mail** > **OK**.

Publikowanie alertów dotyczących programu Operations Manager

1. W Konsola administratora programu DPM kliknij pozycję **monitorowanie** > **akcji** > **Opcje**.
2. W obszarze Opcje kliknij pozycję **Publikowanie alertów** > **Publikowanie aktywnych alertów**.
3. Po włączeniu opcji **Publikowanie alertów** wszystkie istniejące alerty programu DPM, które mogą wymagać reakcji użytkownika, są publikowane w dzienniku zdarzeń **Alerty programu DPM**. Agent programu Operations Manager, który został zainstalowany na serwerze programu DPM, publikuje te alerty w programie Operations Manager i aktualizuje konsolę w miarę generowania nowych alertów.

Odzyskiwanie danych programu Exchange

Odzyskiwanie pojedynczej skrzynki pocztowej

1. Na chronionym serwerze Exchange musi istnieć baza danych skrzynek pocztowych odzyskiwania. Jeśli nie istnieje, utwórz ją przy użyciu polecenia cmdlet New-MailboxDatabase. Przy użyciu polecenia cmdlet Set-MailboxDatabase skonfiguruj możliwość zastąpienia bazy danych odzyskiwania. Na przykład:

```
New-MailboxDatabase -Recovery -Name RDB-CONTROL -Server E2K13-MBX1
```

```
Set-MailboxDatabase -Identity 'RDB-CONTROL' -AllowFileRestore $true
```

2. W Konsoli administratora programu DPM przejdź do widoku **Odzyskiwanie**, a następnie do bazy danych skrzynek pocztowych, która ma zostać odzyskana (w węźle **Wszystkie chronione dane Exchange**).

3. Dostępne punkty odzyskiwania są zaznaczone w kalendarzu i sekcji punktów odzyskiwania pogrubioną czcionką. Kliknij datę, wybierz punkt odzyskiwania w polu **Godzina odzyskiwania** > **Odzyskaj**.

Zwróć uwagę, że nie można wybrać opcji **Najnowszy**. Nie jest ona dostępna dla pojedynczych skrzynek pocztowych.

4. W Kreatorze odzyskiwania sprawdź wybrane odzyskiwanie, a następnie kliknij przycisk **Dalej**.
5. Określ typ odzyskiwania, które chcesz przeprowadzić, a następnie kliknij przycisk **Dalej**.
6. Na stronie **Określ opcje odzyskiwania** wybierz następujące ustawienia:
 - a. **Zainstaluj odzyskane bazy danych**. Usuń zaznaczenie tego pola wyboru, aby nie instalować baz danych.
 - b. **Ograniczenie przepustowości**. Kliknij przycisk **Modyfikuj**, aby włączyć ograniczenie przepustowości.
 - c. Kliknij opcję **Włącz odzyskiwanie na podstawie SAN z użyciem migawek sprzętowych**, jeśli ma zastosowanie.
 - d. W polu **Powiadomienie** kliknij opcję **Wyślij wiadomość e-mail po zakończeniu odzyskiwania** i podaj adresatów. Kolejne adresy e-mail oddziel przecinkami.
7. Na stronie **Podsumowanie** przejrzyj ustawienia odzyskiwania, a następnie kliknij przycisk **Odzyskaj**. Po zakończeniu odzyskiwania kliknij przycisk **Zamknij**.

W trakcie odzyskiwania zostaną anulowane wszystkie zadania synchronizacji dla wybranego elementu odzyskiwania.

8. Po zakończeniu procesu odzyskiwania skrzynka pocztowa nie jest jeszcze całkowicie przywrócona. Baza danych, w której znajduje się ta skrzynka pocztowa, została przywrócona tylko do bazy danych skrzynek pocztowych Przywracanie. Przywróć skrzynkę pocztową, uruchamiając polecenie cmdlet:

```
New-MailboxRestoreRequest -SourceDatabase 'RDB-CONTROL' -SourceStoreMailbox 'mailbox name' -  
TargetMailbox <name>@contoso.com -TargetRootFolder Recovery -SkipMerging StorageProviderForSource
```

Do polecenia należy dodać element `\-SkipMerging StorageProviderForSource`; w przeciwnym razie wystąpi błąd. Aby zapoznać się z obejściem, zobacz informacje o wersji dla programów Exchange 2013 i Exchange 2016.

Gdy otworzysz teraz skrzynkę pocztową `<mailbox name>`, cała jej zawartość sprzed godziny 15:15 będzie znajdować się w folderze Odzyskiwanie.

9. Po zakończeniu przywracania możesz odinstalować i usunąć bazę danych skrzynek pocztowych Odzyskiwanie, uruchamiając następujące polecenie cmdlet programu Windows PowerShell.

```
Remove-MailboxDatabase -Identity 'RDB-CONTROL'
```

Odzyskiwanie bazy danych programu Exchange

- W Konsoli administratora programu DPM przejdź do widoku **Odzyskiwanie**, a następnie do bazy danych skrzynek pocztowych, która ma zostać odzyskana (w węźle **Wszystkie chronione dane Exchange**).
- Dostępne punkty odzyskiwania są zaznaczone w kalendarzu i sekcji punktów odzyskiwania pogrubioną czcionką. Kliknij datę i wybierz opcję **Najnowszy**, aby uzyskać najnowszą kopię zapasową, a następnie kliknij przycisk **Odzyskaj**.
- W Kreatorze odzyskiwania sprawdź wybrane odzyskiwanie, a następnie kliknij przycisk **Dalej**.

- Określ typ odzyskiwania, które chcesz przeprowadzić, a następnie kliknij przycisk **Dalej**.
- Na stronie **Określ opcje odzyskiwania** wybierz następujące ustawienia:
 1. **Zainstaluj odzyskane bazy danych**. Zaznacz tę opcję.
 2. **Ograniczenie przepustowości**. Kliknij przycisk **Modyfikuj**, aby włączyć ograniczenie przepustowości.
 3. Kliknij opcję **Włącz odzyskiwanie na podstawie SAN z użyciem migawek sprzętowych**, jeśli ma zastosowanie.
 4. W polu **Powiadomienie** kliknij opcję **Wyślij wiadomość e-mail po zakończeniu odzyskiwania** i podaj adresatów. Kolejne adresy e-mail oddziel przecinkami.
- Wróć teraz do serwera Exchange i włącz możliwość zastąpienia baz danych przez przywrócenie. Jeśli pominiesz ten krok, przywracanie nie uda się. W tym celu otwórz Centrum administracyjne Exchange, przejdź do opcji **Serwery > Bazy danych**, wybierz bazę danych skrzynek pocztowych, która ma zostać zastąpiona, a następnie kliknij przycisk **Edytuj**.

Kliknij pozycję **konserwacja > Ta baza danych może zostać zastąpiona przez Przywracanie > Zapisz**.

- Wróć do Kreatora odzyskiwania i na stronie **Podsumowanie** przejrzyj ustawienia odzyskiwania, a następnie kliknij przycisk **Odzyskaj**. Po zakończeniu odzyskiwania kliknij przycisk **Zamknij**.

W trakcie odzyskiwania zostaną anulowane wszystkie zadania synchronizacji dla wybranego elementu odzyskiwania.

- Sprawdź zawartość skrzynki pocztowej, aby zweryfikować powodzenie operacji przywracania. Jeśli odzyskana baza danych skrzynek pocztowych należała do grupy dostępności bazy danych (DAG), dla kopii pasywnej widoczny jest stan niepowodzenia i wstrzymania.
- Aby przywrócić normalne działanie grupy DAG, wybierz kopię bazy danych ze stanem niepowodzenia, a następnie kliknij przycisk **Wznów**. Zostanie wyświetlone okno dialogowe z pytaniem o ponowne zainicjowanie (lub zresetowanie) bazy danych. Kliknij przycisk **Tak**.

Odzyskaj cały serwer Exchange Server

- W Konsoli administratora programu DPM przejdź do widoku **Odzyskiwanie**, a następnie do serwera, który ma zostać odzyskany.
- Dostępne punkty odzyskiwania są zaznaczone w kalendarzu i sekcji punktów odzyskiwania pogrubioną czcionką. Kliknij datę i wybierz punkt odzyskiwania z listy. Na liście kliknij prawym przyciskiem myszy pozycję **Odzyskiwanie bez systemu operacyjnego** i kliknij przycisk **Odzyskaj**.
- W Kreatorze odzyskiwania sprawdź wybrane odzyskiwanie, a następnie kliknij przycisk **Dalej**.
- Na stronie **Wybierz typ odzyskiwania** wybierz opcję **Kopiuj do folderu sieciowego**, aby przywrócić serwer do odrębnej lokalizacji sieciowej. Możesz też wybrać opcję **Kopiuj na taśmę**, jeśli jest dostępna.
- Na stronie **Określ miejsce docelowe** wybierz miejsce, do którego chcesz skopiować pliki bazy danych. Przy użyciu tych plików można przeprowadzić odzyskiwanie systemu od zera.
- Na stronie **Określ opcje odzyskiwania** wybierz następujące ustawienia:
 1. **Zainstaluj odzyskane bazy danych**. Zaznacz tę opcję.
 2. **Ograniczenie przepustowości**. Kliknij przycisk **Modyfikuj**, aby włączyć ograniczenie przepustowości.
 3. Kliknij opcję **Włącz odzyskiwanie na podstawie SAN z użyciem migawek sprzętowych**, jeśli ma zastosowanie.

4. W polu **Powiadomienie** kliknij opcję **Wyślij wiadomość e-mail po zakończeniu odzyskiwania** i podaj adresatów. Kolejne adresy e-mail oddziel przecinkami.

- Możesz monitorować ten proces na karcie **monitorowanie**. Po zakończeniu odzyskiwania zostanie wyświetlony alert "powodzenie odzyskiwania".

Otwórz folder, w którym znajdują się pliki odzyskiwania, i zmień jego nazwę na krótszą. Ułatwi to proces odzyskiwania. Utwórz udział w folderze odzyskiwania.

- Aby uruchomić odzyskiwanie systemu od zera, włóż obraz ISO systemu operacyjnego w celu uruchomienia komputera. Wybierz opcję **Napraw** i w sekcji **Opcje zaawansowane** wybierz polecenie **Odzyskiwanie obrazu systemu**.

W kreatorze **Ponowne instalowanie obrazu komputera** możesz zignorować ostrzeżenia o niezalezieniu obrazu systemu.

- Na stronie **Wybierz kopię zapasową obrazu systemu** kliknij pozycję **Wybierz obraz systemu**. Kliknij pozycję **Zaawansowane**, aby wybrać pliki odzyskiwania z udziału sieciowego. Wybierz opcję **Wyszukaj obraz systemu w sieci** i kliknij przycisk **tak**, jeśli pojawi się monit, jeśli masz pewność, że chcesz nawiązać połączenie z siecią.
- Wskaż folder sieciowy, wybierz kopię zapasową i wybierz datę i godzinę obrazu, który chcesz przywrócić. Określ wszystkie dodatkowe ustawienia sterowników i dysków, a następnie kliknij przycisk **Zakończ**, aby rozpocząć przywracanie.

Program System Center Data Protection Manager (DPM) umożliwia tworzenie kopii zapasowych i odzyskiwanie dla programów Exchange 2016 i Exchange 2019. Aby zapewnić ochronę całego wdrożenia programu Exchange, należy skonfigurować ochronę woluminów, stanu systemu lub odzyskiwania pełnego systemu operacyjnego. Ten artykuł zawiera instrukcje dotyczące konfigurowania programu DPM, aby można było chronić wdrożenie programu Exchange. Jeśli masz duże wdrożenie programu Exchange, Użyj grupy dostępności bazy danych (DAG) do skalowania ochrony baz danych skrzynek pocztowych programu Exchange. Aby w pełni chronić wdrożenie programu Exchange, oprócz tworzenia kopii zapasowych baz danych poczty należy utworzyć kopie zapasowe ról programu Exchange Server, takich jak serwer dostępu klienta lub usługa transportu na serwerach skrzynek pocztowych.

Wymagania wstępne i ograniczenia

Przed wdrożeniem programu DPM w celu ochrony programów Exchange 2016 i Exchange 2019 Sprawdź wymagania wstępne dotyczące wdrażania:

- Przeglądnij [Informacje o wersji programu DPM](#)
- Zapoznaj się z artykułem, [co jest obsługiwane i co nie dotyczy programu DPM?](#), w przypadku jakichkolwiek problemów z programem Exchange.
- Upewnij się, że zarówno na serwerze programu Exchange, jak i na serwerze programu DPM zostały zainstalowane te same wersje plików Eseutil.exe i Ese.dll. Na przykład jeśli korzystasz z 64-bitowej wersji programu DPM, musisz mieć 64-bitowe wersje plików eseutil.exe i ese.dll. W przypadku aktualizacji tych plików na serwerze Exchange należy również zaktualizować pliki na serwerze programu DPM. Pliki `.ese` i `.eseutil` znajdują się zwykle w lokalizacji, `C:\Program Files\Microsoft\Exchange Server\V15\Bin`.

Aby zachować aktualne kopie:

1. W wierszu polecenia przejdź do katalogu `<DPM installation folder>\Bin`.

2. Wpisz polecenie fsutil w następujący sposób, aby utworzyć twardy link do pliku Eseutil. exe:

```
fsutil hardlink create <link> <target>
```


Na przykład w typowym typie instalacji:

```
fsutil hardlink create "c:\program files\microsoft\dpm\bin\eseutil.exe" "c:\program files\microsoft\Exchange\bin\eseutil.exe"
```

- Zainstaluj [pakiet Visual C++ Redistributable dla programu Visual Studio 2012 Update](#).
- Aby chronić węzeł grupy dostępności bazy danych (DAG) programu Exchange 2016 i programu Exchange 2019, Zainstaluj agenta ochrony programu DPM na węźle. Należy pamiętać, że można chronić różne węzły DAG z różnych serwerów DPM. Tylko jeden węzeł może być chroniony za pomocą tylko jednego serwera DPM.
- Program DPM 2012 (i nowsze) ma limit rozmiaru puli magazynu równy 120 terabajt (TB). Istnieje limit 80 TB dla woluminów repliki programu DPM i limit 40 TB dla woluminów punktów odzyskiwania. W przypadku ochrony dużego wdrożenia programu Exchange należy znać limit rozmiaru skrzynki pocztowej użytkownika oraz liczbę użytkowników lub skrzynek pocztowych. Liczba użytkowników lub skrzynek pocztowych określa maksymalny rozmiar skrzynki pocztowej. Jeśli skrzynki pocztowe pozostają w granicach, Liczba skrzynek pocztowych określa liczbę baz danych programu Exchange, które mogą być chronione przez jeden program DPM. Użyj liczby użytkowników przypisanych do bazy danych i ich limitów skrzynek pocztowych, aby obliczyć maksymalny rozmiar możliwy dla każdej bazy danych programu Exchange. Na przykład jeśli maksymalny rozmiar skrzynki pocztowej użytkownika 8 GB, jeden serwer DPM może chronić do 10 000 skrzynek pocztowych. Jeśli maksymalny rozmiar skrzynki pocztowej użytkownika jest większy niż 8 GB lub w przypadku, gdy więcej niż 10 000 skrzynek pocztowych użytkowników wymaga ochrony, skonfiguruj serwer programu Exchange z DAG. Aby zapewnić pełną ochronę, użyj dodatkowych serwerów programu DPM. Węzeł programu Exchange może być chroniony tylko przez jeden serwer DPM. W związku z tym liczba węzłów programu Exchange powinna być równa lub większa niż liczba serwerów programu DPM wymaganych do ochrony wszystkich baz danych programu Exchange.
- Program DPM działa z dowolną rolą bazy danych. Program DPM można skonfigurować tak, aby chronił serwer hostujący kolekcję aktywnych lub pasywnych baz danych skrzynek pocztowych.
- Skonfiguruj jedną pełną kopię zapasową dziennie i częstotliwość synchronizacji zgodnie z wymaganiami dotyczącymi obciążenia dzienników programu Exchange. W przypadku ochrony więcej niż jednej kopii bazy danych skrzynek pocztowych programu Exchange (na przykład podczas ochrony członków DAG) skonfiguruj jeden węzeł dla pełnych kopii zapasowych i pozostały do kopiowania kopii zapasowych. Kopie kopii zapasowych nie powodują obcinania plików dziennika.
- Chronić co najmniej dwie kopie każdej bazy danych skrzynek pocztowych. Do przechowywania można używać niedrogich dysków Serial Advanced Technology (SATA) lub kilku dysków JBOD.
- Dla synchronizacji skrzynki pocztowej ustaw częstotliwość minimalną na więcej niż 15 minut. Rozpocznij od konfiguracji aktualnych zasad tworzenia kopii zapasowych, a następnie stopniowo zwiększaj liczbę punktów odzyskiwania. Wykonywanie jednego lub dwóch zadań tworzenia ekspresowych pełnych kopii zapasowych dziennie, przy częstotliwości synchronizacji wynoszącej dwie godziny, to rozsądne rozwiązanie. Aby uzyskać optymalną częstotliwość synchronizacji, należy wziąć pod uwagę ilość danych, wpływ na wydajność oraz ilość wymaganą do przechowywania replik.
- Program Exchange 2016 i program Exchange 2019 mogą obsługiwać maksymalnie osiem równoległych kopii zapasowych. Aby obsłużyć zadania tworzenia równoległych kopii zapasowych bazy danych programu Exchange dla serwera Exchange, utwórz wiele grup ochrony (maksymalnie osiem) i dodaj bazy danych programu Exchange do każdej grupy ochrony.
- Zachowując dane programu Exchange, należy pamiętać o następujących kwestiach:
 - **Dodawanie baz danych skrzynek pocztowych do serwera.** W przypadku tworzenia lub dodawania nowych baz danych skrzynek pocztowych do chronionej grupy magazynów na serwerze Exchange te bazy danych są automatycznie dodawane do zadań replikacji i ochrony w programie DPM. Można dodać bazy danych skrzynki pocztowej w trakcie tworzenia przyrostowych kopii

zapasowych dopiero po zakończeniu tworzenia pełnych kopii zapasowych.

- o **Zmiana ścieżek plików bazy danych skrzynek pocztowych.** Jeśli chroniona baza danych lub pliki dziennika zostaną przeniesione do woluminu zawierającego dane chronione za pomocą programu DPM, ochrona będzie kontynuowana. W przypadku przeniesienia chronionej bazy danych lub plików dziennika do woluminu, który nie jest chroniony za pomocą programu DPM, zostanie wyświetlony alert i zadania ochrony zakończą się niepowodzeniem. Aby rozwiązać alert, kliknij link **Modyfikuj zadanie ochrony** w obszarze szczegółów alertu, po czym uruchom sprawdzanie spójności.
- o **Odinstalowywanie baz danych skrzynek pocztowych.** W przypadku odinstalowywania chronionej bazy danych skrzynki pocztowej zadanie ochrony dla tej określonej bazy danych kończy się niepowodzeniem. Replika zostaje oznaczona jako niespójna, gdy program DPM uruchamia kolejne zadanie tworzenia ekspresowej pełnej kopii zapasowej.
- o **Zmiana nazw baz danych skrzynek pocztowych.** Jeśli musisz zmienić nazwę bazy danych skrzynki pocztowej, wyłącz ochronę i włącz ochronę bazy danych ponownie. Przed ponownym włączeniem ochrony bazy danych tworzenie kopii zapasowych jest kontynuowane, ale wyliczanie skrzynki pocztowej kończy się niepowodzeniem.

Dlaczego warto wykonywać kopie zapasowe programu Exchange przy użyciu programu DPM?

Podczas podejmowania decyzji o utworzeniu kopii zapasowej danych programu Exchange przy użyciu programu Exchange 2016 i programu Exchange 2019 Native Data Protection lub DPM należy wziąć pod uwagę następujące kwestie:

Ochrona danych natywnych umożliwia:

- Odzyskiwanie po awarii
- Odzyskiwanie przypadkowo usuniętych elementów
- Przechowywanie danych przez dłuższy okres.
- Tworzenie migawek baz danych z określonego momentu

Ochrona danych natywnych może być mimo tego niewystarczająca, jeśli występują błędy aplikacji, uszkodzenia lub zdarzenia związane z zabezpieczeniami i złośliwym oprogramowaniem. W takich sytuacjach program DPM oferuje następujące korzyści:

- Mniejsza liczba wymaganych grup DAG — ochrona danych natywnych wymaga dodatkowych serwerów skrzynek pocztowych do hostowania kopii aktywnych danych. Tworzenie kopii zapasowych przy użyciu funkcji ochrony programu DPM w żaden sposób nie zależy od grup DAG.
- Prostsze przywracanie — program DPM udostępnia proste i scentralizowane odzyskiwanie danych z kopii zapasowych z określonego punktu w czasie.
- Dłuższy zakres przechowywania — program DPM oferuje dłuższe czasy przechowywania kopii zapasowych danych. Ochrona danych natywnych jest ograniczona do 14 dni.
- Spójne tworzenie kopii zapasowych obciążeń dotyczących rozwiązań firmy Microsoft — program DPM oferuje scentralizowany i prosty proces tworzenia kopii zapasowych danych i ich odzyskiwania dla obciążeń dotyczących rozwiązań firmy Microsoft, w tym programu Exchange, serwerów plików, programu SQL Server, funkcji Hyper-V i programu SharePoint.

Przed rozpoczęciem

1. **Wdrażanie programu DPM** — sprawdź, czy program DPM został poprawnie zainstalowany i wdrożony.

Jeśli nie zostało to jeszcze zrobione, zobacz:

- Wymagania systemowe dotyczące programu DPM
 - [Co program DPM może umieścić w kopii zapasowej?](#)
 - [Elementy obsługiwane i nieobsługiwane przez program DPM](#)
 - [Instalowanie programu DPM](#)
2. Konfigurowanie magazynu — dane kopii zapasowej można przechowywać na dysku, na taśmie i w chmurze przy użyciu platformy Azure. Więcej informacji znajduje się w temacie [Prepare data storage](#) (Przygotowanie magazynu danych).
 3. **Skonfiguruj agenta ochrony DPM** — Agent musi być zainstalowany na serwerze Exchange. Zapoznaj się z tematem [Deploy the DPM protection agent](#) (Wdrażanie agenta ochrony programu DPM).

Konfigurowanie kopii zapasowej

1. Kliknij pozycję **ochrona > Akcje > Utwórz grupę ochrony**, aby otworzyć kreatora **tworzenia nowej grupy ochrony** w konsoli programu DPM.
2. Na stronie **Wybierz typ grupy ochrony** wybierz pozycję **Serwery**.
3. Na stronie **Wybierz członków grupy** wybierz wszystkie grupy DAG zawierające dane, które chcesz chronić. Dla każdego serwera programu Exchange można również wybrać opcję tworzenia kopii zapasowej stanu systemu lub pełnej kopii zapasowej kompletnego stanu systemu (zawierającej dane o stanie systemu). Jest to przydatne, jeśli chcesz mieć możliwość odzyskania całego serwera, a nie tylko danych. [Wdrażanie grup ochrony](#).
4. W obszarze **Wybierz metodę ochrony danych** określ, jak mają być obsługiwane krótkoterminowe i długoterminowe kopie zapasowe. Krótkoterminowa kopia zapasowa jest zawsze najpierw tworzona na dysku z opcją przeniesienia kopii zapasowej z dysku do chmury platformy Azure za pomocą usługi Azure Backup (na potrzeby przechowywania krótkoterminowego lub długoterminowego). Zamiast długoterminowej kopii zapasowej w chmurze możesz również skonfigurować długoterminową kopię zapasową na autonomicznym urządzeniu taśmowym lub w bibliotece taśm połączonej z serwerem programu DPM.
5. Na stronie **Określ opcje ochrony programu Exchange** wybierz pozycję **Uruchom program Eseutil**, aby sprawdzić integralność danych w celu sprawdzenia integralności baz danych programu Exchange. Spowoduje to przeniesienie operacji sprawdzania spójności kopii zapasowej z programu Exchange Server na serwer programu DPM, co oznacza, że wpływ operacji we/wy programu Eseutil.exe na program Exchange Server podczas tworzenia kopii zapasowej zostanie wyeliminowany. Aby chronić grupę DAG, upewnij się, że wybierasz opcję Uruchom tylko dla plików dziennika (zalecane dla serwerów DAG). Jeśli plik eseutil nie został wcześniej skopiowany, wystąpi błąd.
6. Na stronie **Określ ochronę Exchange DAG** wybierz bazy danych, które chcesz skopiować w postaci pełnej kopii zapasowej lub kopii kopii zapasowej, korzystając z list **Kopie bazy danych wybrane do pełnej kopii zapasowej** lub **Kopie bazy danych wybrane do kopii zapasowej**. W celu ochrony wielu kopii tej samej bazy danych można wybrać tylko jedną kopię dla pełnej kopii zapasowej, a następnie wybrać pozostałe kopie jako kopie kopii zapasowej.
7. W polu **Wybierz cele krótkoterminowe** określ sposób tworzenia kopii zapasowej w krótkoterminowym magazynie na dysku. W obszarze **Zakres przechowywania** określ, jak długo chcesz przechowywać dane na dysku. W obszarze **Częstotliwość synchronizacji** określ, jak często chcesz zapisywać przyrostowe kopie zapasowe na dysku. Jeśli nie chcesz ustawiać interwału kopii zapasowych, możesz sprawdzić tuż przed punktem odzyskiwania, aby program DPM wykonał ekspresową pełną kopię zapasową tuż przed

zaplanowaniem każdego punktu odzyskiwania.

8. Jeśli chcesz utworzyć długoterminową kopię zapasową danych na taśmie, na stronie **Określ cele długoterminowe** wskaż, jak długo chcesz przechowywać dane na taśmie (od 1 roku do 99 lat). W obszarze Częstotliwość wykonywania kopii zapasowych określ, jak często mają być wykonywane kopie zapasowe na taśmie. Częstotliwość zależy od wybranego zakresu przechowywania:

- Gdy zakres przechowywania wynosi 1–99 lat, można wybrać tworzenie kopii zapasowej codziennie, co tydzień, co dwa tygodnie, co miesiąc, co kwartał, co pół roku lub co rok.
- Gdy zakres przechowywania wynosi 1–11 miesięcy, można wybrać tworzenie kopii zapasowej codziennie, co tydzień, co dwa tygodnie lub co miesiąc.
- Gdy zakres przechowywania wynosi 1–4 tygodnie, można wybrać tworzenie kopii zapasowej codziennie lub co tydzień.

W przypadku korzystania z autonomicznej stacji taśm dla pojedynczej grupy ochrony program DPM używa tej samej taśmy do codziennego wykonywania kopii zapasowych do momentu, gdy zabraknie na niej miejsca. Na taśmie można również zapisywać dane z różnych grup ochrony.

Na stronie **Określanie szczegółów taśmy i biblioteki** określ taśmę lub bibliotekę, która ma być używana, oraz czy dane na taśmie mają być kompresowane i szyfrowane.

9. Na stronie **Przejrzyj przydział dysku** przejrzyj miejsce na dysku w puli magazynów przydzielone danej grupie ochrony.

Całkowity rozmiar danych to rozmiar danych, dla których ma zostać utworzona kopia zapasowa, a w obszarze **Miejsce na dysku do udostępnienia w programie DPM** jest widoczna ilość miejsca zalecana przez program DPM dla grupy ochrony. Program DPM wybierze idealną wielkość kopii zapasowej na podstawie ustawień. Opcje wielkości kopii zapasowej można jednak edytować w obszarze **Szczegóły przydziału dysku**. W przypadku obciążeń wybierz z menu rozwijanego preferowany magazyn. Edycja zmienia wartości pozycji **Całkowita ilość miejsca dla magazynu i Wolne miejsce w magazynie** w okienku **Dostępny magazyn dyskowy**. Miejsce poniżej aprowizacji to ilość miejsca, które program DPM sugeruje dodać do woluminu, aby bezproblemowo wykonywać kopie zapasowe w przyszłości.

10. W polu **Wybierz metodę tworzenia repliki** określ, jak chcesz obsługiwać początkową pełną replikację danych. W przypadku wybrania replikowania za pośrednictwem sieci zaleca się wybranie czasu w godzinach małego obciążenia sieci. W przypadku dużych ilości danych lub nieoptymalnych warunków sieciowych należy wziąć pod uwagę replikację danych w trybie offline za pomocą nośników wymiennych.
11. W polu **Wybierz opcje sprawdzania spójności** wybierz sposób automatyzacji sprawdzania spójności. Można włączyć uruchamianie sprawdzania tylko wtedy, gdy dane są niespójne, lub zgodnie z harmonogramem. Jeśli nie chcesz konfigurować automatycznego sprawdzania spójności, w dowolnym momencie możesz uruchomić sprawdzanie ręczne, klikając prawym przyciskiem myszy grupę ochrony w obszarze **Ochrona** w konsoli programu DPM i wybierając polecenie **Przeprowadź sprawdzanie spójności**.
12. Jeśli wybrano opcję tworzenia kopii zapasowych w chmurze przy użyciu usługi Azure Backup, sprawdź, czy na stronie **Określanie danych chronionych w trybie online** zaznaczono obciążenia, dla których ma być tworzona kopia zapasowa na platformie Azure.
13. W obszarze **Określanie harmonogramu tworzenia kopii zapasowych online** określ, jak często mają być wykonywane przyrostowe kopie zapasowe na platformie Azure. Wykonywanie kopii zapasowych można zaplanować na każdy dzień/tydzień/miesiąc/rok, natomiast godziny/daty pozwalają ustalić konkretny czas uruchomienia wykonywania kopii zapasowych. Kopie zapasowe mogą być tworzone maksymalnie dwa razy dziennie. Zawsze podczas wykonywania kopii zapasowej na platformie Azure jest tworzony punkt odzyskiwania danych na podstawie kopii danych przechowywanych w kopii zapasowej na dysku programu

DPM.

14. W polu **Określ zasady przechowywania danych online** możesz określić sposób przechowywania na platformie Azure punktów odzyskiwania tworzonych na podstawie kopii zapasowych wykonywanych co dzień/tydzień/miesiąc/rok.
15. W polu **Wybierz replikację online** określ, jak będzie wykonywana początkowa pełna replikacja danych. Możesz wykonywać replikację za pośrednictwem sieci lub tworzyć kopie zapasowe offline (rozmieszczanie offline). W przypadku kopii zapasowych offline używana jest funkcja Azure Import. [Przeczytaj więcej](#).
16. Na stronie **Podsumowanie** przejrzyj ustawienia. Po kliknięciu pozycji **Utwórz grupę** następuje początkowa replikacja danych. Po ukończeniu replikacji grupa ochrony będzie mieć stan **OK** na stronie **Stan**. Następnie odbywa się tworzenie kopii zapasowych zgodnie z ustawieniami grupy ochrony.

Monitorowanie

Po utworzeniu grupy ochrony następuje replikacja początkowa i program DPM rozpoczyna wykonywanie kopii zapasowej i synchronizowanie danych programu Exchange. Program DPM monitoruje synchronizację początkową i tworzenie kolejnych kopii zapasowych. Możesz monitorować dane programu Exchange na kilka sposobów:

- Za pomocą domyślnej funkcji monitorowania programu DPM można skonfigurować powiadomienia na potrzeby aktywnego monitorowania (przez publikowanie alertów i konfigurowanie powiadomień). Powiadomienia mogą być przesyłane pocztą e-mail w przypadku alertów krytycznych, ostrzeżeń lub informacji oraz w przypadku informacji o stanie wystąpień procesu odzyskiwania.
- Korzystając z programu Operations Manager, można publikować alerty z poziomu centralnej lokalizacji.

Konfigurowanie powiadomień dotyczących monitorowania

1. W Konsola administratora programu DPM kliknij pozycję **monitorowanie** > **akcji** > **Opcje**.
2. Kliknij pozycję **Serwer SMTP**, a następnie wpisz nazwę serwera, port i adres e-mail, z którego będą wysyłane powiadomienia. Adres musi być prawidłowy.
3. W obszarze **uwierzytelniony serwer SMTP** wpisz nazwę użytkownika i hasło. Nazwa użytkownika i hasło muszą odpowiadać nazwie konta domeny należącego do osoby, której adres „Od” został opisany w poprzednim kroku. W przeciwnym razie dostarczanie powiadomień nie powiedzie się.
4. Aby przetestować ustawienia serwera SMTP, kliknij pozycję **Wyślij testową wiadomość e-mail**, wpisz adres e-mail, na który serwer programu DPM ma przesłać wiadomość testową, a następnie kliknij przycisk **OK**. Kliknij kolejno pozycje **Opcje** > **Powiadomienia**, a następnie wybierz typy alertów, o których odbiorcy chcą być powiadamiani. W polu **Odbiorcy** wpisz adres e-mail każdego odbiorcy, do którego program DPM ma przysyłać kopie powiadomień.
5. Aby przetestować ustawienia serwera SMTP, kliknij pozycję **Wyślij testowe powiadomienie e-mail** > **OK**.

Publikowanie alertów dotyczących programu Operations Manager

1. W Konsola administratora programu DPM kliknij pozycję **monitorowanie** > **akcji** > **Opcje**.
2. W obszarze Opcje kliknij pozycję **Publikowanie alertów** > **Publikowanie aktywnych alertów**.
3. Po włączeniu opcji **Publikowanie alertów** wszystkie istniejące alerty programu DPM, które mogą wymagać reakcji użytkownika, są publikowane w dzienniku zdarzeń **Alerty programu DPM**. Agent programu Operations Manager, który został zainstalowany na serwerze programu DPM, publikuje te alerty w programie Operations Manager i aktualizuje konsolę w miarę generowania nowych alertów.

Odzyskiwanie danych programu Exchange

Odzyskiwanie pojedynczej skrzynki pocztowej

1. Na chronionym serwerze Exchange musi istnieć baza danych skrzynek pocztowych odzyskiwania. Jeśli nie istnieje, utwórz ją przy użyciu polecenia cmdlet `New-MailboxDatabase`. Przy użyciu polecenia cmdlet `Set-MailboxDatabase` skonfiguruj możliwość zastąpienia bazy danych odzyskiwania. Na przykład:

```
New-MailboxDatabase -Recovery -Name RDB-CONTROL -Server E2K13-MBX1
```

```
Set-MailboxDatabase -Identity 'RDB-CONTROL' -AllowFileRestore $true
```

2. W Konsoli administratora programu DPM przejdź do widoku **Odzyskiwanie**, a następnie do bazy danych skrzynek pocztowych, która ma zostać odzyskana (w węźle **Wszystkie chronione dane Exchange**).

3. Dostępne punkty odzyskiwania są zaznaczone w kalendarzu i sekcji punktów odzyskiwania pogrubioną czcionką. Kliknij datę, wybierz punkt odzyskiwania w polu **Godzina odzyskiwania** > **Odzyskaj**.

Zwróć uwagę, że nie można wybrać opcji **Najnowszy**. Nie jest ona dostępna dla pojedynczych skrzynek pocztowych.

4. W Kreatorze odzyskiwania sprawdź wybrane odzyskiwanie, a następnie kliknij przycisk **Dalej**.
5. Określ typ odzyskiwania, które chcesz przeprowadzić, a następnie kliknij przycisk **Dalej**.
6. Na stronie **Określ opcje odzyskiwania** wybierz następujące ustawienia:
 - a. **Zainstaluj odzyskane bazy danych**. Usuń zaznaczenie tego pola wyboru, aby nie instalować baz danych.
 - b. **Ograniczenie przepustowości**. Kliknij przycisk **Modyfikuj**, aby włączyć ograniczenie przepustowości.
 - c. Kliknij opcję **Włącz odzyskiwanie na podstawie SAN z użyciem migawek sprzętowych**, jeśli ma zastosowanie.
 - d. W polu **Powiadomienie** kliknij opcję **Wyślij wiadomość e-mail po zakończeniu odzyskiwania** i podaj adresatów. Kolejne adresy e-mail oddziel przecinkami.
7. Na stronie **Podsumowanie** przejrzyj ustawienia odzyskiwania, a następnie kliknij przycisk **Odzyskaj**. Po zakończeniu odzyskiwania kliknij przycisk **Zamknij**.

W trakcie odzyskiwania zostaną anulowane wszystkie zadania synchronizacji dla wybranego elementu odzyskiwania.

8. Po zakończeniu procesu odzyskiwania skrzynka pocztowa nie jest jeszcze całkowicie przywrócona. Baza danych, w której znajduje się ta skrzynka pocztowa, została przywrócona tylko do bazy danych skrzynek pocztowych Przywracanie. Przywróć skrzynkę pocztową, uruchamiając polecenie cmdlet:

```
New-MailboxRestoreRequest -SourceDatabase 'RDB-CONTROL' -SourceStoreMailbox 'mailbox name' -  
TargetMailbox <name>@contoso.com -TargetRootFolder Recovery -SkipMerging StorageProviderForSource
```

Do polecenia należy dodać element `\-SkipMerging StorageProviderForSource`; w przeciwnym razie wystąpi błąd. Aby zapoznać się z obejściem, zobacz informacje o wersji dla programów Exchange 2016 i Exchange 2019.

Gdy otworzysz teraz skrzynkę pocztową `<mailbox name>`, cała jej zawartość sprzed godziny 15:15 będzie znajdować się w folderze Odzyskiwanie.

9. Po zakończeniu przywracania możesz odinstalować i usunąć bazę danych skrzynek pocztowych **Odzyskiwanie**, uruchamiając następujące polecenie cmdlet programu Windows PowerShell.

```
Remove-MailboxDatabase -Identity 'RDB-CONTROL'
```

Odzyskiwanie bazy danych programu Exchange

- W Konsoli administratora programu DPM przejdź do widoku **Odzyskiwanie**, a następnie do bazy danych skrzynek pocztowych, która ma zostać odzyskana (w węźle **Wszystkie chronione dane Exchange**).
- Dostępne punkty odzyskiwania są zaznaczone w kalendarzu i sekcji punktów odzyskiwania pogrubioną czcionką. Kliknij datę i wybierz opcję **Najnowszy**, aby uzyskać najnowszą kopię zapasową, a następnie kliknij przycisk **Odzyskaj**.
- W Kreatorze odzyskiwania sprawdź wybrane odzyskiwanie, a następnie kliknij przycisk **Dalej**.
- Określ typ odzyskiwania, które chcesz przeprowadzić, a następnie kliknij przycisk **Dalej**.
- Na stronie **Określ opcje odzyskiwania** wybierz następujące ustawienia:

1. **Zainstaluj odzyskane bazy danych**. Zaznacz tę opcję.
2. **Ograniczenie przepustowości**. Kliknij przycisk **Modyfikuj**, aby włączyć ograniczenie przepustowości.
3. Kliknij opcję **Włącz odzyskiwanie na podstawie SAN z użyciem migawek sprzętowych**, jeśli ma zastosowanie.
4. W polu **Powiadomienie** kliknij opcję **Wyślij wiadomość e-mail po zakończeniu odzyskiwania** i podaj adresatów. Kolejne adresy e-mail oddziel przecinkami.

- Wróć teraz do serwera Exchange i włącz możliwość zastąpienia baz danych przez przywrócenie. Jeśli pominiesz ten krok, przywracanie nie uda się. W tym celu otwórz Centrum administracyjne Exchange, przejdź do opcji **Serwery > Bazy danych**, wybierz bazę danych skrzynek pocztowych, która ma zostać zastąpiona, a następnie kliknij przycisk **Edytuj**.

Kliknij pozycję **konserwacja > Ta baza danych może zostać zastąpiona przez Przywracanie > Zapisz**.

- Wróć do Kreatora odzyskiwania i na stronie **Podsumowanie** przejrzyj ustawienia odzyskiwania, a następnie kliknij przycisk **Odzyskaj**. Po zakończeniu odzyskiwania kliknij przycisk **Zamknij**.

W trakcie odzyskiwania zostaną anulowane wszystkie zadania synchronizacji dla wybranego elementu odzyskiwania.

- Sprawdź zawartość skrzynki pocztowej, aby zweryfikować powodzenie operacji przywracania. Jeśli odzyskana baza danych skrzynek pocztowych należała do grupy dostępności bazy danych (DAG), dla kopii pasywnej widoczny jest stan niepowodzenia i wstrzymania.
- Aby przywrócić normalne działanie grupy DAG, wybierz kopię bazy danych ze stanem niepowodzenia, a następnie kliknij przycisk **Wznów**. Zostanie wyświetlone okno dialogowe z pytaniem o ponowne zainicjowanie (lub zresetowanie) bazy danych. Kliknij przycisk **Tak**.

Odzyskaj cały serwer Exchange Server

- W Konsoli administratora programu DPM przejdź do widoku **Odzyskiwanie**, a następnie do serwera, który ma zostać odzyskany.
- Dostępne punkty odzyskiwania są zaznaczone w kalendarzu i sekcji punktów odzyskiwania pogrubioną czcionką. Kliknij datę i wybierz punkt odzyskiwania z listy. Na liście kliknij prawym przyciskiem myszy pozycję **Odzyskiwanie bez systemu operacyjnego** i kliknij przycisk **Odzyskaj**.

- W Kreatorze odzyskiwania sprawdź wybrane odzyskiwanie, a następnie kliknij przycisk **Dalej**.
- Na stronie **Wybierz typ odzyskiwania** wybierz opcję **Kopiuj do folderu sieciowego**, aby przywrócić serwer do odrębnej lokalizacji sieciowej. Możesz też wybrać opcję **Kopiuj na taśmę**, jeśli jest dostępna.
- Na stronie **Określ miejsce docelowe** wybierz miejsce, do którego chcesz skopiować pliki bazy danych. Przy użyciu tych plików można przeprowadzić odzyskiwanie systemu od zera.
- Na stronie **Określ opcje odzyskiwania** wybierz następujące ustawienia:
 1. **Zainstaluj odzyskane bazy danych**. Zaznacz tę opcję.
 2. **Ograniczenie przepustowości**. Kliknij przycisk **Modyfikuj**, aby włączyć ograniczenie przepustowości.
 3. Kliknij opcję **Włącz odzyskiwanie na podstawie SAN z użyciem migawek sprzętowych**, jeśli ma zastosowanie.
 4. W polu **Powiadomienie** kliknij opcję **Wyślij wiadomość e-mail po zakończeniu odzyskiwania** i podaj adresatów. Kolejne adresy e-mail oddziel przecinkami.
- Możesz monitorować ten proces na karcie **monitorowanie**. Po zakończeniu odzyskiwania zostanie wyświetlony alert "powodzenie odzyskiwania".

Otwórz folder, w którym znajdują się pliki odzyskiwania, i zmień jego nazwę na krótszą. Ułatwi to proces odzyskiwania. Utwórz udział w folderze odzyskiwania.

- Aby uruchomić odzyskiwanie systemu od zera, włóż obraz ISO systemu operacyjnego w celu uruchomienia komputera. Wybierz opcję **Napraw** i w sekcji **Opcje zaawansowane** wybierz polecenie **Odzyskiwanie obrazu systemu**.

W kreatorze **Ponowne instalowanie obrazu komputera** możesz zignorować ostrzeżenia o nieznalezieniu obrazu systemu.

- Na stronie **Wybierz kopię zapasową obrazu systemu** kliknij pozycję **Wybierz obraz systemu**. Kliknij pozycję **Zaawansowane**, aby wybrać pliki odzyskiwania z udziału sieciowego. Wybierz opcję **Wyszukaj obraz systemu w sieci** i kliknij przycisk **tak**, jeśli pojawi się monit, jeśli masz pewność, że chcesz nawiązać połączenie z siecią.
- Wskaż folder sieciowy, wybierz kopię zapasową i wybierz datę i godzinę obrazu, który chcesz przywrócić. Określ wszystkie dodatkowe ustawienia sterowników i dysków, a następnie kliknij przycisk **Zakończ**, aby rozpocząć przywracanie.

Tworzenie kopii zapasowej programu SharePoint przy użyciu programu DPM

10.01.2020 • 34 minutes to read

Program System Center Data Protection Manager (DPM) można wdrożyć w celu ochrony Farm programu SharePoint, zewnętrznych baz danych SQL Server i folderów, które obejmują dostosowania farmy. W tym artykule opisano czynności, które należy wykonać, aby utworzyć kopię zapasową danych programu SharePoint i odzyskać te dane. Uzupełnieniem tego artykułu są poniższe wpisy na blogu, które zawierają szczegółowy instruktaż i porady w zakresie rozwiązywania problemów dotyczących tego scenariusza:

- [Configure SharePoint protection in DPM \(Konfigurowanie ochrony programu SharePoint w programie DPM\)](#)
- [Backing up and troubleshooting SharePoint and DPM \(Wykonywanie kopii zapasowych i rozwiązywanie problemów związanych z programami SharePoint i DPM\)](#)
- [Restoring SharePoint with DPM \(Przywracanie programu SharePoint przy użyciu programu DPM\)](#)

Wymagania wstępne i ograniczenia

- Aby uzyskać listę obsługiwanych wersji programu SharePoint i wersji programu DPM wymaganych do wykonywania kopii zapasowych poszczególnych wersji programu SharePoint, zobacz artykuł [What can DPM back up?](#) (Kopie zapasowe wykonywane przez program DPM).
- Ochrona programu SharePoint obejmuje domyślnie wszystkie bazy danych zawartości (oraz bazy danych SharePoint_Config i SharePoint_AdminContent*). Jeśli chcesz dodać dostosowania, takie jak indeksy wyszukiwania, usługa profilu użytkownika, szablony lub bazy danych usługi aplikacji, musisz oddzielnie skonfigurować je pod kątem ochrony. Upewnij się, że ochrona została włączona dla wszystkich folderów zawierających te typy funkcji lub pliki dostosowań.
- Bazy danych programu SharePoint korzystające z funkcji AlwaysOn mogą być chronione od wersji programu DPM 2012 R2 z dodatkiem Update 5 lub nowszym.
- Nie można włączyć ochrony baz danych programu SharePoint jako źródła danych programu SQL Server. Z kopii zapasowej farmy można odzyskiwać pojedyncze bazy danych.
- Aby program DPM wykonywał kopie zapasowe baz danych programu SQL Server przy użyciu konta System lokalny, konto to musi mieć uprawnienia administratora systemu dla programu SQL Server. Na serwerze programu SQL Server, którego kopię zapasową chcesz wykonać, ustaw uprawnienia administratora systemu dla konta ZARZĄDZANIE NT\SYSTEM.
- Dla każdego 10 milionów elementów w farmie musi istnieć co najmniej 2 GB miejsca na woluminie, w którym znajduje się folder programu DPM. Miejsce to jest wymagane na potrzeby generowania wykazów. Aby umożliwić użycie programu DPM w celu przeprowadzenia odzyskiwania na poziomie elementu (zbiory witryn, witryny, listy, biblioteki dokumentów, foldery, pojedyncze dokumenty i elementy list), funkcja generowania wykazu tworzy listę adresów URL przechowywanych w poszczególnych bazach danych zawartości. Listę tych adresów URL można zobaczyć w okienku elementów możliwych do odzyskania znajdującym się w obszarze zadania Odzyskiwanie w konsoli administratora programu DPM.
- Jeśli w farmie programu SharePoint znajdują się bazy danych programu SQL Server, które skonfigurowano z użyciem aliasów programu SQL Server, zainstaluj składniki klienckie tego programu na serwerze frontonu sieci Web, który ma być chroniony przez program DPM.

- Ochrona elementów sklepu z aplikacjami nie jest obsługiwana w programie SharePoint 2013.
- Program DPM nie obsługuje ochrony zdalnego katalogu FILESTREAM. Katalog FILESTREAM powinien być częścią bazy danych.

Przed rozpoczęciem

1. **Wdrażanie programu DPM** — sprawdź, czy program DPM został poprawnie zainstalowany i wdrożony. Jeśli nie zostało to jeszcze zrobione, zobacz:
 - Wymagania systemowe dotyczące programu DPM
 - [Co program DPM może umieścić w kopii zapasowej?](#)
 - [Elementy obsługiwane i nieobsługiwane przez program DPM](#)
 - [Instalowanie programu DPM](#)
2. **Konfigurowanie magazynu** — dane kopii zapasowej można przechowywać na dysku, na taśmie i w chmurze przy użyciu platformy Azure. Więcej informacji znajduje się w temacie [Prepare data storage](#) (Przygotowanie magazynu danych).
3. **Konfigurowanie agenta ochrony programu DPM** — agenta ochrony programu DPM należy zainstalować na każdym serwerze w farmie programu SharePoint, łącznie z serwerami programu SQL Server. Jedynym wyjątkiem jest zainstalowanie go tylko na jednym serwerze frontonu sieci Web (WFE). Jeśli na przykład masz jedną farmę z dwoma serwerami WFE, serwerem indeksowania i dwuwęzłowym klastrem programu SQL Server, musisz zainstalować agenta na serwerze indeksowania, obu węzłach klastra programu SQL Server oraz jednym serwerze WFE. Ponieważ serwery WFE nie hostują zawartości, agent służący jako punkt wejścia ochrony jest potrzebny tylko na jednym serwerze WFE. Zapoznaj się z tematem [Deploy the DPM protection agent](#) (Wdrażanie agenta ochrony programu DPM).

Jeśli program SharePoint korzysta z bazy danych programu SQL Server, która znajduje się na zdalnym komputerze, musisz skonfigurować na nim agenta programu DPM. Jeśli baza danych znajduje się w klastrze, zainstaluj agenta we wszystkich węzłach klastra.

Konfigurowanie kopii zapasowej

Aby utworzyć kopię zapasową farmy programu SharePoint, skonfiguruj ochronę programu SharePoint przy użyciu pliku ConfigureSharePoint.exe, a następnie utwórz grupę ochrony w programie DPM.

1. **Uruchom narzędzie ConfigureSharePoint.exe** — służy ono do konfigurowania usługi składnika zapisywania usługi VSS dla programu SharePoint (WSS) i udostępnia agentowi ochrony poświadczenia dla farmy programu SharePoint. Po wdrożeniu agenta ochrony plik ConfigureSharePoint.exe można znaleźć w folderze <ścieżka instalacji programu DPM>\bin na serwerze frontonu-sieci Web. Jeśli masz wiele serwerów WFE, zainstaluj go tylko na jednym z nich. Postępuj w następujący sposób:
 - Na serwerze WFE w wierszu polecenia przejdź do <lokalizacji instalacji programu DPM>\bin\ i uruchom **ConfigureSharePoint [-EnableSharePointProtection] [-EnableSPSearchProtection] [-ResolveAllSQLAliases] [-SetTempPath]**, gdzie:
 - **EnableSharePointProtection** włącza ochronę farmy programu SharePoint i składnik zapisywania usługi VSS oraz rejestruje tożsamość aplikacji DCOM WssCmdletsWrapper w celu uruchomienia jej jako użytkownik, którego poświadczenia wprowadzono przy użyciu tej opcji. To konto powinno należeć do grupy administratorów farmy oraz administratorów lokalnych serwera frontonu sieci Web.
 - **EnableSPSearchProtection** włącza ochronę usługi WSS 3.0 SP Search przy użyciu klucza rejestru SharePointSearchEnumerationEnabled w gałęzi HKLM\Software\Microsoft\Microsoft

Data Protection Manager\Agent\2.0\ z przodu- na serwerze frontonu sieci Web i rejestruje tożsamość aplikacji DCOM WssCmdletsWrapper w celu uruchomienia jej jako użytkownika, którego poświadczenia wprowadzono przy użyciu tej opcji. To konto powinno należeć do grupy administratorów farmy oraz administratorów lokalnych serwera frontonu sieci Web.

- **ResolveAllSQLAliases** wyświetla wszystkie aliasy raportowane przez składnik zapisywania usługi VSS programu SharePoint i rozpoznaje je jako odpowiednie serwery programu SQL Server. Wyświetla również rozpoznane nazwy wystąpień. Serwery zdublowane również zostaną wyświetlone. Raportuje wszystkie aliasy nierozpoznane jako serwer programu SQL Server.
- **SetTempPath** ustawia zmienne środowiskowe TEMP i TMP na określoną ścieżkę. Jeśli jest odzyskiwany duży zbiór witryn, witryna, lista lub element, a w folderze tymczasowym administratora farmy jest zbyt mało miejsca, odzyskiwanie na poziomie elementu nie powiedzie się. Ta opcja pozwala zmienić ścieżkę folderu plików tymczasowych na wolumin, który ma wystarczająco dużo miejsca, aby zmieścić odzyskiwany zbiór witryn lub witrynę.
- Wprowadź poświadczenia administratora farmy. To konto musi należeć do lokalnej grupy administratorów na serwerze WFE. Jeśli administrator farmy nie jest administratorem lokalnym, przyznaj następujące uprawnienia na serwerze WFE:
 - Grupie WSS_Admin_WPG przyznaj pełną kontrolę nad folderem programu DPM (%Program Files%\Microsoft Data Protection Manager\DPM). -A
 - Grupie WSS_Admin_WPG przyznaj dostęp do odczytu klucza rejestru programu DPM (HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft Data Protection Manager).

Plik ConfigureSharePoint.exe musisz uruchomić ponownie w przypadku zmiany poświadczeń administratora farmy programu SharePoint.

2. W celu utworzenia grupy ochrony kliknij kolejno pozycje **Ochrona > Akcje > Utwórz grupę ochrony**, aby otworzyć kreatora **tworzenia nowej grupy ochrony** w konsoli programu DPM.
3. Na stronie **Wybierz typ grupy ochrony** wybierz pozycję **Serwery**.
4. W obszarze **Wybierz członków grupy** rozwiń serwer, który pełni rolę serwera WFE. Jeśli istnieje więcej niż jeden serwer WFE, wybierz ten, na którym zainstalowano plik ConfigureSharePoint.exe. Aby dowiedzieć się więcej, zobacz [Deploy protection groups](#) (Wdrażanie grup ochrony).

Po rozwinięciu serwera programu SharePoint program DPM wysyła zapytanie do usługi VSS, aby sprawdzić, jakie dane mogą być chronione. Jeśli baza danych programu SharePoint jest zdalna, program DPM nawiąże z nią połączenie. Jeśli źródła danych programu SharePoint nie pojawią się, sprawdź, czy na serwerze programu SharePoint i jakimkolwiek zdalnym serwerze programu SQL Server jest uruchomiony składnik zapisywania usługi VSS. Upewnij się również, że zarówno na serwerze programu SharePoint, jak i zdalnym serwerze programu SQL Server jest zainstalowany agent programu DPM. Ponadto upewnij się, że bazy danych programu SharePoint nie są chronione w innym miejscu jako bazy danych programu SQL Server.

5. W obszarze **Wybierz metodę ochrony danych** określ, jak mają być obsługiwane krótkoterminowe i długoterminowe kopie zapasowe. Krótkoterminowa kopia zapasowa jest zawsze najpierw tworzona na dysku z opcją przeniesienia kopii zapasowej z dysku do chmury Azure za pomocą usługi Azure Backup (na potrzeby przechowywania krótkoterminowego i długoterminowego). Zamiast długoterminowej kopii zapasowej w chmurze możesz również skonfigurować długoterminową kopię zapasową na standardowym urządzeniu taśmowym lub w bibliotece taśm podłączonej do serwera programu DPM.
6. Na stronie **Wybierz cele krótkoterminowe** określ sposób tworzenia kopii zapasowej w krótkoterminowym magazynie na dysku. W obszarze **Zakres przechowywania** określ, jak długo chcesz

przechowywać dane na dysku. W obszarze **Częstotliwość synchronizacji** określ, jak często chcesz zapisywać przyrostowe kopie zapasowe na dysku. Jeśli nie chcesz ustawiać interwału kopii zapasowych, możesz zaznaczyć opcję Zaraz przed punktem odzyskiwania, aby program DPM wykonywał ekspresową pełną kopię zapasową bezpośrednio przed każdym zaplanowanym punktem odzyskiwania.

7. Jeśli chcesz utworzyć długoterminową kopię zapasową danych na taśmie, na stronie **Określ cele długoterminowe** wskaż, jak długo chcesz przechowywać dane na taśmie (od 1 roku do 99 lat). W obszarze **Częstotliwość wykonywania kopii zapasowych** określ, jak często mają być wykonywane kopie zapasowe na taśmie. Częstotliwość zależy od wybranego zakresu przechowywania:

- Gdy zakres przechowywania wynosi 1–99 lat, można wybrać tworzenie kopii zapasowej codziennie, co tydzień, co dwa tygodnie, co miesiąc, co kwartał, co pół roku lub co rok.
- Gdy zakres przechowywania wynosi 1–11 miesięcy, można wybrać tworzenie kopii zapasowej codziennie, co tydzień, co dwa tygodnie lub co miesiąc.
- Gdy zakres przechowywania wynosi 1–4 tygodnie, można wybrać tworzenie kopii zapasowej codziennie lub co tydzień.

W przypadku korzystania z autonomicznej stacji taśm dla pojedynczej grupy ochrony program DPM używa tej samej taśmy do codziennego wykonywania kopii zapasowych do momentu, gdy zabraknie na niej miejsca. Na taśmie można również zapisywać dane z różnych grup ochrony.

Na stronie **Określanie szczegółów taśmy i biblioteki** określ taśmę lub bibliotekę, która ma być używana, oraz czy dane na taśmie mają być kompresowane i szyfrowane.

8. Na stronie **Przejrzyj przydział dysku** przejrzyj miejsce na dysku w puli magazynów przydzielone danej grupie ochrony.

Całkowity rozmiar danych to rozmiar danych, dla których ma zostać utworzona kopia zapasowa, a w obszarze **Miejsce na dysku do udostępnienia w programie DPM** jest widoczna ilość miejsca zalecana przez program DPM dla grupy ochrony. Program DPM wybierze idealną wielkość kopii zapasowej na podstawie ustawień. Opcje wielkości kopii zapasowej można jednak edytować w obszarze **Szczegóły przydziału dysku**. W przypadku obciążeń wybierz z menu rozwijanego preferowany magazyn. Edycja zmienia wartości pozycji **Całkowita ilość miejsca dla magazynu** i **Wolne miejsce w magazynie** w okienku **Dostępny magazyn dyskowy**. Miejsce poniżej apro wizacji to ilość miejsca, które program DPM sugeruje dodać do woluminu, aby bezproblemowo wykonywać kopie zapasowe w przyszłości.

9. W polu **Wybierz metodę tworzenia repliki** określ, jak chcesz obsługiwać początkową pełną replikację danych. W przypadku wybrania replikowania za pośrednictwem sieci zaleca się wybranie czasu w godzinach małego obciążenia sieci. W przypadku dużych ilości danych lub nieoptymalnych warunków sieciowych należy wziąć pod uwagę replikację danych w trybie offline za pomocą nośników wymiennych.
10. W polu **Wybierz opcje sprawdzania spójności** wybierz sposób automatyzacji sprawdzania spójności. Można włączyć uruchamianie sprawdzania tylko wtedy, gdy dane są niespójne, lub zgodnie z harmonogramem. Jeśli nie chcesz konfigurować automatycznego sprawdzania spójności, w dowolnym momencie możesz uruchomić sprawdzanie ręczne, klikając prawym przyciskiem myszy grupę ochrony w obszarze **Ochrona** w konsoli programu DPM i wybierając polecenie **Przeprowadź sprawdzanie spójności**.
11. Jeśli wybrano opcję tworzenia kopii zapasowych w chmurze przy użyciu usługi Azure Backup, sprawdź, czy na stronie **Określanie danych chronionych w trybie online** zaznaczono obciążenia, dla których ma być tworzona kopia zapasowa na platformie Azure.
12. W obszarze **Określanie harmonogramu tworzenia kopii zapasowych online** określ, jak często mają być wykonywane przyrostowe kopie zapasowe na platformie Azure. Wykonywanie kopii zapasowych można zaplanować na każdy dzień/tydzień/miesiąc/rok, natomiast godziny/daty pozwalają ustalić konkretny czas

uruchomienia wykonywania kopii zapasowych. Kopie zapasowe mogą być tworzone maksymalnie dwa razy dziennie. Zawsze podczas wykonywania kopii zapasowej na platformie Azure jest tworzony punkt odzyskiwania danych na podstawie kopii danych przechowywanych w kopii zapasowej na dysku programu DPM.

13. W polu **Określ zasady przechowywania danych online** możesz określić sposób przechowywania na platformie Azure punktów odzyskiwania tworzonych na podstawie kopii zapasowych wykonywanych co dzień/tydzień/miesiąc/rok.
14. W polu **Wybierz replikację online** określ, jak będzie wykonywana początkowa pełna replikacja danych. Możesz wykonywać replikację za pośrednictwem sieci lub tworzyć kopie zapasowe offline (rozmieszczanie offline). W przypadku kopii zapasowych offline używana jest funkcja Azure Import. [Przeczytaj więcej](#).
15. Na stronie **Podsumowanie** przejrzyj ustawienia. Po kliknięciu pozycji **Utwórz grupę** następuje początkowa replikacja danych. Po ukończeniu replikacji grupa ochrony będzie mieć stan **OK** na stronie **Stan**. Następnie odbywa się tworzenie kopii zapasowych zgodnie z ustawieniami grupy ochrony.

Monitorowanie

Po utworzeniu grupy ochrony następuje replikacja początkowa i program DPM rozpoczyna wykonywanie kopii zapasowej i synchronizowanie danych programu Exchange. Program DPM monitoruje synchronizację początkową i tworzenie kolejnych kopii zapasowych. Możesz monitorować dane programu SharePoint na kilka sposobów:

- Za pomocą domyślnej funkcji monitorowania programu DPM można skonfigurować powiadomienia na potrzeby aktywnego monitorowania (przez publikowanie alertów i konfigurowanie powiadomień). Powiadomienia mogą być przesyłane pocztą e-mail w przypadku alertów krytycznych, ostrzeżeń lub informacji oraz w przypadku informacji o stanie wystąpień procesu odzyskiwania.
- Korzystając z programu Operations Manager, można publikować alerty z poziomu centralnej lokalizacji.

Konfigurowanie powiadomień dotyczących monitorowania

1. W konsoli administratora programu DPM kliknij kolejno pozycje **Monitorowanie** > **Akcja** > **Opcje**.
2. Kliknij pozycję **Serwer SMTP**, a następnie wpisz nazwę serwera, port i adres e-mail, z którego będą wysyłane powiadomienia. Adres musi być prawidłowy.
3. W obszarze **Uwierzytelniony serwer SMTP** wpisz nazwę użytkownika i hasło. Nazwa użytkownika i hasło muszą odpowiadać nazwie konta domeny należącego do osoby, której adres „Od” został opisany w poprzednim kroku. W przeciwnym razie dostarczanie powiadomień nie powiedzie się.
4. Aby przetestować ustawienia serwera SMTP, kliknij pozycję **Wyślij testową wiadomość e-mail**, wpisz adres e-mail, na który serwer programu DPM ma przesłać wiadomość testową, a następnie kliknij przycisk **OK**. Kliknij kolejno pozycje **Opcje** > **Powiadomienia**, a następnie wybierz typy alertów, o których odbiorcy chcą być powiadamiani. W polu **Odbiorcy** wpisz adres e-mail każdego odbiorcy, do którego program DPM ma przysyłać kopie powiadomień.

Publikowanie alertów dotyczących programu Operations Manager

1. W konsoli administratora programu DPM kliknij kolejno pozycje **Monitorowanie** > **Akcja** > **Opcje** > **Publikowanie alertów** > **Publikuj aktywne alerty**.
2. Po włączeniu opcji **Publikowanie alertów** wszystkie istniejące alerty programu DPM, które mogą wymagać reakcji użytkownika, są publikowane w dzienniku zdarzeń **Alerty programu DPM**. Agent programu Operations Manager, który został zainstalowany na serwerze programu DPM, publikuje te alerty w programie Operations Manager i aktualizuje konsolę w miarę generowania nowych alertów.

Przywracanie danych programu SharePoint

Dane programu SharePoint można odzyskać w następujący sposób:

- Odzyskiwanie do lokalizacji oryginalnej
- Odzyskiwanie do innej lokalizacji. Należy zauważyć, że nie można wykonać odzyskiwania pełnej farmy do nowej lokalizacji.
- Kopiowanie danych do folderu sieciowego
- Kopiowanie danych na taśmę

W celu odzyskania farmy należy pamiętać o następujących kwestiach:

- Jeśli serwer programu SharePoint jest chroniony jako baza danych programu SQL Server, można odzyskać dane programu SharePoint, wybierając bazę danych programu SQL Server w Kreatorze odzyskiwania.
- W celu odzyskania farmy należy pamiętać o następujących kwestiach:
 - Serwery frontonu sieci Web powinny być skonfigurowane tak samo, jak podczas tworzenia punktu odzyskiwania.
 - Na serwerze frontonu sieci Web musi zostać utworzona struktura farmy. Dane farmy zostaną odzyskane do istniejącej struktury.
 - Wystąpienia programu SQL Server powinny być skonfigurowane przy użyciu takich samych nazw, jak podczas tworzenia punktu odzyskiwania.
 - Wystąpienia programu SQL Server powinny być skonfigurowane przy użyciu takiej samej konfiguracji dysków, jak podczas tworzenia punktu odzyskiwania.
 - W farmie podstawowej farmy odzyskiwania muszą być zainstalowane wszystkie dodatki Service Pack, pakiety językowe i poprawki.
 - Nie należy próbować bezpośrednio odzyskiwać bazy danych zawartości centralnej lokacji administracyjnej lub bazy danych konfiguracji, ponieważ może to spowodować uszkodzenie danych w farmie programu SharePoint.
 - Godzina punktu odzyskiwania danych programu SharePoint wyświetlana na karcie **przeglądanie** może się różnić od godziny wyświetlanej na karcie **Wyszukiwanie**. Na karcie **przeglądanie** zostanie wyświetlony czas tworzenia kopii zapasowej farmy, a na karcie **Wyszukiwanie** wyświetlana jest poprawna godzina punktu odzyskiwania dla witryn, dokumentów i folderów.

Istnieje kilka możliwych scenariuszy odzyskiwania farmy:

- Konfiguracja farmy istnieje, tak jak w czasie wykonywania kopii zapasowej. W takim przypadku odzyskiwanie zostanie wykonane do działającej farmy.
- Baza danych konfiguracji jest uszkodzona, a serwery farmy nie działają.

Odzyskiwanie danych do działającej farmy

1. W konsoli administratora programu DPM kliknij na pasku nawigacyjnym opcję **Odzyskiwanie**.
2. W okienku **Chronione dane** rozwiń serwer zawierający farmę, którą chcesz odzyskać, a następnie kliknij pozycję **Wszystkie chronione dane SharePoint**. W okienku wyników **Element możliwy do odzyskania** nazwa farmy jest wyświetlana w formacie nazwa serwera\nazwa farmy.
3. W kalendarzu kliknij dowolną pogrubioną datę, aby pobrać listę punktów odzyskiwania dostępnych dla tej daty. W menu **Godzina odzyskiwania** są wyświetlane godziny poszczególnych dostępnych punktów odzyskiwania.
4. W menu **Godzina odzyskiwania** wybierz punkt odzyskiwania, którego chcesz użyć.

5. W okienku **Akcje** kliknij polecenie **Odzyskaj**.

Zostanie uruchomiony Kreator odzyskiwania.

6. Na stronie **Przegląd wybranego elementu do odzyskania** kliknij przycisk **Dalej**.

7. Wybierz lokalizację, do której chcesz odzyskać bazę danych. Należy pamiętać o następujących kwestiach:

- Nie można odzyskać całej farmy do innej lokalizacji.
- Jeśli wybierzesz opcję **Kopiuj do folderu sieciowego**, a wybrany punkt odzyskiwania nie został utworzony przy użyciu funkcji ekspresowej pełnej kopii zapasowej, zostaną wyświetlone nowe opcje punktu odzyskiwania.
- Jeśli wybierzesz opcję **Kopiuj na taśmę**, a wybrany punkt odzyskiwania nie został utworzony przy użyciu funkcji ekspresowej pełnej kopii zapasowej, zostaną wyświetlone nowe opcje punktu odzyskiwania. W przypadku opcji taśmy należy wybrać bibliotekę taśm, która ma zostać użyta do odzyskiwania.

8. Określ opcje odzyskiwania dotyczące ograniczania przepustowości sieci, odzyskiwania wykorzystującego sieć SAN i powiadomień e-mail, a następnie kliknij przycisk **Dalej**.

9. Na stronie **Podsumowanie** przejrzyj ustawienia odzyskiwania, a następnie kliknij przycisk **Odzyskaj**.

Odzyskiwanie danych do niedziałającej farmy

1. Utwórz nową farmę, która używa tego samego wystąpienia programu SQL Server i tego samego serwera frontonu sieci Web co oryginalna chroniona farma.

2. Na serwerze frontonu sieci Web używanym przez program DPM do odzyskiwania danych farmy uruchom następujące polecenie w wierszu poleceń: `ConfigureSharePoint-EnableSharePointProtection`

3. W konsoli administratora programu DPM kliknij na pasku nawigacyjnym opcję **Odzyskiwanie**.

4. W okienku **Chronione dane** rozwiń serwer zawierający farmę, którą chcesz odzyskać, a następnie kliknij pozycję **Wszystkie chronione dane SharePoint**. W okienku wyników **Element możliwy do odzyskania** nazwa farmy jest wyświetlana w formacie nazwa serwera\nazwa farmy.

5. W kalendarzu kliknij dowolną pogrubioną datę, aby pobrać listę punktów odzyskiwania dostępnych dla tej daty. W menu **Godzina odzyskiwania** są wyświetlane godziny poszczególnych dostępnych punktów odzyskiwania.

6. W menu **Godzina odzyskiwania** wybierz punkt odzyskiwania, którego chcesz użyć.

7. W okienku **Akcje** kliknij polecenie **Odzyskaj**.

Zostanie uruchomiony Kreator odzyskiwania.

8. Na stronie **Przegląd wybranego elementu do odzyskania** kliknij przycisk **Dalej**.

9. Wybierz lokalizację, do której chcesz odzyskać bazę danych. Należy pamiętać o następujących kwestiach:

- Nie można odzyskać całej farmy do innej lokalizacji.
- Jeśli wybierzesz opcję **Kopiuj do folderu sieciowego**, a wybrany punkt odzyskiwania nie został utworzony przy użyciu funkcji ekspresowej pełnej kopii zapasowej, zostaną wyświetlone nowe opcje punktu odzyskiwania.
- Jeśli wybierzesz opcję **Kopiuj na taśmę**, a wybrany punkt odzyskiwania nie został utworzony przy użyciu funkcji ekspresowej pełnej kopii zapasowej, zostaną wyświetlone nowe opcje punktu odzyskiwania. W przypadku opcji taśmy należy wybrać bibliotekę taśm, która ma zostać użyta do odzyskiwania.

10. Określ opcje odzyskiwania dotyczące ograniczania przepustowości sieci, odzyskiwania wykorzystującego sieć SAN i powiadomień e-mail, a następnie kliknij przycisk **Dalej**.
11. Na stronie **Podsumowanie** przejrzyj ustawienia odzyskiwania, a następnie kliknij przycisk **Odzyskaj**.
12. Na głównym serwerze frontonu sieci Web farmy serwerów uruchom Kreatora konfiguracji produktów i technologii programu SharePoint i odłącz serwer frontonu sieci Web od farmy.

Przełączanie serwera frontonu sieci Web

Poniższa procedura używa przykładu farmy serwerów z dwoma serwerami frontonu sieci Web, serwer1 i serwer2. Program DPM używa serwer1 do ochrony farmy. Należy zmienić serwer frontonu sieci Web, z którego korzysta program DPM, aby można było usunąć serwer1 z farmy.

NOTE

Jeśli serwer frontonu sieci Web używany przez program DPM do ochrony farmy jest niedostępny, użyj poniższej procedury, aby zmienić serwer frontonu sieci Web, rozpoczynając od kroku 4.

Aby zmienić serwer frontonu sieci Web, którego program DPM używa do ochrony farmy

1. Zatrzymaj usługę składnika zapisywania usługi VSS programu SharePoint na serwerze Serwer1, uruchamiając następujące polecenie w wierszu polecenia:

stsadm -o unregisterwsswriter

2. Na serwerze Serwer1 Otwórz Edytor rejestru i przejdź do następującego klucza:

HKLM\System\CCS\Services\VSS\VssAccessControl

3. Zaznacz wszystkie wartości wymienione w podkluczu VssAccessControl. Jeśli dowolny wpis ma dane wartości 0 i inny składnik zapisywania usługi VSS jest uruchomiony w ramach poświadczeń skojarzonego konta, Zmień dane wartości na 1.
4. Zainstaluj agenta ochrony na serwerze serwer2.

WARNING

Można przełączyć tylko serwery frontonu sieci Web, jeśli oba serwery znajdują się w tej samej domenie.

5. Na serwerze Serwer2 w wierszu polecenia Zmień katalog na *lokalizację instalacji programu DPM\Bin* i uruchom polecenie ConfigureSharepoint. Aby uzyskać więcej informacji na temat ConfigureSharePoint, zobacz [Konfigurowanie kopii zapasowej](#).
6. Występuje znany problem, gdy farma serwerów jest jedynym członkiem grupy ochrony, a grupa ochrony jest skonfigurowana do korzystania z ochrony opartej na taśmach. Jeśli farma serwerów jest jedynym członkiem grupy ochrony przy użyciu ochrony opartej na taśmach, aby zmienić serwer frontonu sieci Web używany przez program DPM do ochrony farmy, należy tymczasowo dodać innego członka do grupy ochrony, wykonując następujące czynności:
 - W konsoli administratora programu DPM kliknij opcję **Ochrona** na pasku nawigacyjnym.
 - Wybierz grupę ochrony, do której należy farma serwerów, a następnie kliknij przycisk **Modyfikuj grupę ochrony**.
 - W Kreatorze modyfikowania grupy Dodaj wolumin na dowolnym serwerze do grupy ochrony. Po zakończeniu procedury można usunąć ten wolumin z ochrony.

- Jeśli grupa ochrony jest skonfigurowana do krótkoterminowej ochrony opartej na dyskach i długoterminowej ochrony opartej na taśmach, wybierz opcję ręcznego tworzenia repliki. Pozwala to uniknąć tworzenia repliki dla woluminu, który jest tymczasowo dodawany do grupy ochrony.
- Ukończ pracę kreatora.

7. Usuń serwer serwer1 z grupy ochrony, wybierając opcję zachowania replik na dysku i taśmie.
8. Wybierz grupę ochrony, do której należy farma serwerów, a następnie kliknij przycisk **Modyfikuj grupę ochrony**.
9. W Kreatorze modyfikowania grupy na stronie **Wybierz członków grupy** rozwiń węzeł Serwer2 i wybierz farmę serwerów, a następnie Ukończ pracę kreatora.

Zostanie uruchomione sprawdzanie spójności.

10. Jeśli wykonano krok 6, można teraz usunąć wolumin z grupy ochrony.

Tworzenie kopii zapasowych programu SQL Server za pomocą programu DPM

28.02.2020 • 31 minutes to read

Program System Center Data Protection Manager (DPM) udostępnia kopie zapasowe i odzyskiwanie dla SQL Server baz danych. Oprócz tworzenia kopii zapasowych baz danych programu SQL Server można wykonywać kopie zapasowe systemu lub pełne kopie zapasowe kompletnego stanu komputera z programem SQL Server. Oto konfiguracje, które mogą być chronione przez program DPM:

- Autonomiczne wystąpienie programu SQL Server
- Wystąpienie klastra trybu failover (FCI) programu SQL Server
- Grupa dostępności AlwaysOn programu SQL Server z następującymi preferencjami:
 - Tylko pomocnicza
 - Główna
 - Dowolna replika

Dlaczego warto tworzyć kopie zapasowe programu SQL Server za pomocą programu DPM?

- Program DPM zaprojektowano tak, aby chronić zaawansowane konfiguracje programu SQL Server.
- Program DPM można ustawić tak, aby program SQL Server był chroniony nawet co 15 minut.
- Program DPM zmniejsza ryzyko potencjalnych konfliktów między narzędziami do tworzenia kopii zapasowych i harmonogramami ochrony programu SQL Server.
- Program DPM może chronić program SQL Server na poziomie wystąpienia lub bazy danych. Po włączeniu ochrony na poziomie wystąpienia program DPM wykrywa nowe bazy danych w tym wystąpieniu i automatycznie dodaje je do grupy ochrony.
- Program DPM jest przystępny cenowo. Świetnie sprawdza się w przypadku niewielkiego rozmiaru bazy danych SQL Server i można go skalować na potrzeby organizacji z bazami danych SQL Server o większych rozmiarach.
- Program DPM zawiera narzędzie do samoobsługowego odzyskiwania (SSRT), które rozszerza opcje administratorów bazy danych umożliwiające samoobsługowe odzyskiwanie baz danych SQL.
- Po uaktualnieniu programu SQL Server do wersji 2014 wykonywanie kopii zapasowych baz danych, które są już chronione przez program DPM, będzie kontynuowane. Podczas uaktualniania programu SQL Server nie należy uruchamiać zadań tworzenia kopii zapasowych.

Wymagania wstępne i ograniczenia

- Jeśli Twoja baza danych ma pliki w zdalnym udziale plików, ochrona zakończy się niepowodzeniem z błędem o identyfikatorze 104. Program DPM nie obsługuje ochrony danych programu SQL Server w zdalnym udziale plików.
- Program DPM nie chroni baz danych przechowywanych w zdalnych udziałach SMB.

- Należy się upewnić, że repliki grupy dostępności są skonfigurowane jako przeznaczone tylko do odczytu.
- W programie SQL Server należy jawnie dodać konto systemowe Zarządzanie NT\System do grupy administratorów systemu.
- W przypadku przeprowadzania odzyskiwania do lokalizacji alternatywnej dla częściowo zawartej bazy danych należy dopilnować, aby docelowe wystąpienie programu SQL Server miało włączoną funkcję Zawarte bazy danych.
- Ochrona programu SQL Server z włączoną funkcją AlwaysOn:
 - Program DPM wykrywa grupy dostępności podczas uruchamiania zapytań w trakcie tworzenia grupy ochrony.
 - Program DPM wykrywa tryb failover i nadal chroni bazę danych.
 - Program DPM obsługuje konfigurację klastra wielolokalizacyjnego dla wystąpienia programu SQL Server.

W przypadku ochrony baz danych używających funkcji AlwaysOn program DPM ma następujące ograniczenia:

- Program DPM uznaje zasadę tworzenia kopii zapasowej dla grup dostępności, które są ustawione w programie SQL Server, na podstawie następujących preferencji tworzenia kopii zapasowej:
 - Preferuj pomocniczą — kopie zapasowe będą stosowane tylko do repliki pomocniczej z wyjątkiem sytuacji, gdy replika podstawowa jest jedyną repliką online. Jeśli jest dostępnych wiele replik pomocniczych, do kopii zapasowej zostanie wybrany węzeł o najwyższym priorytecie kopii zapasowej. Jeśli jest dostępna tylko replika podstawowa, do kopii zapasowej zostaje wybrana replika podstawowa.
 - Tylko pomocnicza — kopia zapasowa nie powinna być wykonywana dla repliki podstawowej. Jeśli replika podstawowa jest jedyną repliką online, kopia zapasowa nie powinna być wykonywana.
 - Podstawowa — kopie zapasowe powinny być zawsze wykonywane dla repliki podstawowej.
 - Dowolna replika — kopie zapasowe powinny być wykonywane dla dowolnych replik w grupie dostępności. Węzeł, z którego będzie wykonywana kopia zapasowa, powinien być oparty na priorytetach kopii zapasowej dla każdego z węzłów.
- Należy pamiętać o następujących kwestiach:
 - Kopie zapasowe mogą być tworzone z dowolnej możliwej do odczytu repliki, tj. podstawowej, synchronicznej pomocniczej i asynchronicznej pomocniczej.
 - Jeśli jakkolwiek replika zostanie wykluczona z kopii zapasowej, gdy na przykład będzie włączona opcja Wyklucz replikę lub replika jest oznaczona jako nie do odczytu, wówczas ta replika nie zostanie wybrana do kopii zapasowej bez względu na preferencje.
 - Jeśli jest dostępnych i możliwych do odczytu wiele replik, wtedy do kopii zapasowej zostanie wybrany węzeł o najwyższym priorytecie kopii zapasowej.
 - Jeśli tworzenie kopii zapasowej dla wybranego węzła nie powiedzie się, operacja wykonywania kopii zapasowej zakończy się niepowodzeniem.
 - Odzyskiwanie do oryginalnej lokalizacji nie jest obsługiwane.
- Problemy z kopiami zapasowymi programu SQL Server 2014:
 - W programie SQL Server 2014 dodano nową funkcję umożliwiającą tworzenie bazy danych

lokalnego programu SQL Server w usłudze Windows Azure Blob Storage. Program DPM nie obsługuje ochrony tej konfiguracji.

- o Znane są problemy dotyczące użycia ustawienia „Preferuj pomocniczą” z opcją AlwaysOn programu SQL Server — program DPM zawsze wykonuje kopię zapasową na podstawie pomocniczej bazy danych, a jeśli pomocnicza baza danych nie zostanie znaleziona, tworzenie kopii zapasowej nie powiedzie się.

Przed rozpoczęciem

1. **Wdrażanie programu DPM** — sprawdź, czy program DPM został poprawnie zainstalowany i wdrożony. Jeśli nie zostało to jeszcze zrobione, zobacz:
 - Wymagania systemowe dotyczące programu DPM
 - [Co program DPM może umieścić w kopii zapasowej?](#)
 - [Elementy obsługiwane i nieobsługiwane przez program DPM](#)
 - [Instalowanie programu DPM](#)
2. **Konfigurowanie magazynu** — dane kopii zapasowej można przechowywać na dysku, na taśmie i w chmurze przy użyciu platformy Azure. Więcej informacji znajduje się w temacie [Prepare data storage](#) (Przygotowanie magazynu danych).
3. **Konfigurowanie agenta ochrony programu DPM** — agenta ochrony programu DPM należy zainstalować na każdym komputerze, dla którego mają być tworzone kopie zapasowe. Zapoznaj się z tematem [Deploy the DPM protection agent](#) (Wdrażanie agenta ochrony programu DPM).

Konfigurowanie kopii zapasowej

1. W celu utworzenia grupy ochrony kliknij kolejno pozycje **Ochrona** > **Akcje** > **Utwórz grupę ochrony**, aby utworzyć kreatora **tworzenia nowej grupy ochrony** w konsoli programu DPM.
2. W obszarze **Wybierz typ grupy ochrony** wybierz pozycję **Serwery**.
3. W obszarze **Wybierz członków grupy** wybierz wystąpienia programu SQL Server na serwerze, który chcesz chronić. Aby dowiedzieć się więcej, zobacz [Deploy protection groups](#) (Wdrażanie grup ochrony). Należy pamiętać o następujących kwestiach:
 - Istnieje możliwość wyboru ochrony na poziomie wystąpienia ochrony pojedynczych baz danych.
 - W przypadku ochrony na poziomie wystąpienia wszystkie bazy danych dodane do wystąpienia programu SQL Server zostaną automatycznie dodane do ochrony programu DPM.
 - Jeśli są używane grupy dostępności AlwaysOn programu SQL Server, można utworzyć grupę ochrony zawierającą te grupy dostępności. Program DPM wykrywa grupy dostępności i wyświetla je w obszarze **Grupa klastra**. Wybierz całą grupę, aby zapewnić automatyczną ochronę każdej bazy danych dodawanej do tej grupy, lub wybierz poszczególne bazy danych. Dla każdego wystąpienia programu SQL Server można również uruchomić tworzenie kopii zapasowej stanu systemu lub kopii zapasowej całego systemu. Jest to przydatne, jeśli chcesz mieć możliwość odzyskania całego serwera, a nie tylko danych.
4. W obszarze **Wybierz metodę ochrony danych** określ, jak mają być obsługiwane krótkoterminowe i długoterminowe kopie zapasowe. Krótkoterminowa kopia zapasowa jest zawsze najpierw tworzona na dysku z opcją przeniesienia kopii zapasowej z dysku do chmury platformy Azure za pomocą usługi Azure Backup (na potrzeby przechowywania krótkoterminowego lub długoterminowego). Zamiast długoterminowej kopii zapasowej w chmurze możesz również skonfigurować długoterminową kopię

zapasową na autonomicznym urządzeniu taśmowym lub w bibliotece taśm połączonej z serwerem programu DPM.

5. W obszarze **Wybierz cele krótkoterminowe** określ sposób tworzenia kopii zapasowej w krótkoterminowym magazynie na dysku. W obszarze **Zakres przechowywania** określ, jak długo chcesz przechowywać dane na dysku. W obszarze **Częstotliwość synchronizacji** określ, jak często chcesz zapisywać przyrostowe kopie zapasowe na dysku. Jeśli nie chcesz ustawiać interwału kopii zapasowych, możesz wybrać pozycję **Zaraz przed punktem odzyskiwania**, aby program DPM wykonywał ekspresową pełną kopię zapasową bezpośrednio przed każdym zaplanowanym punktem odzyskiwania.

6. Jeśli chcesz utworzyć długoterminową kopię zapasową danych na taśmie, w obszarze **Określ cele długoterminowe** wskaż, jak długo chcesz przechowywać dane na taśmie (od 1 roku do 99 lat). W obszarze **Częstotliwość wykonywania kopii zapasowych** określ, jak często mają być wykonywane kopie zapasowe na taśmie. Częstotliwość zależy od wybranego zakresu przechowywania:

- Gdy zakres przechowywania wynosi 1–99 lat, można wybrać tworzenie kopii zapasowej codziennie, co tydzień, co dwa tygodnie, co miesiąc, co kwartał, co pół roku lub co rok.
- Gdy zakres przechowywania wynosi 1–11 miesięcy, można wybrać tworzenie kopii zapasowej codziennie, co tydzień, co dwa tygodnie lub co miesiąc.
- Gdy zakres przechowywania wynosi 1–4 tygodnie, można wybrać tworzenie kopii zapasowej codziennie lub co tydzień.

W przypadku korzystania z autonomicznej stacji taśm dla pojedynczej grupy ochrony program DPM używa tej samej taśmy do codziennego wykonywania kopii zapasowych do momentu, gdy zabraknie na niej miejsca. Na taśmie można również zapisywać dane z różnych grup ochrony.

Na stronie **Określanie szczegółów taśmy i biblioteki** określ taśmę lub bibliotekę, która ma być używana, oraz czy dane na taśmie mają być kompresowane i szyfrowane.

7. Na stronie **Przejrzyj przydział dysku** przejrzyj miejsce na dysku w puli magazynów przydzielone danej grupie ochrony.

Całkowity rozmiar danych to rozmiar danych, dla których ma zostać utworzona kopia zapasowa, a w obszarze **Miejsce na dysku do udostępnienia w programie DPM** jest widoczna ilość miejsca zalecana przez program DPM dla grupy ochrony. Program DPM wybierze idealną wielkość kopii zapasowej na podstawie ustawień. Opcje wielkości kopii zapasowej można jednak edytować w obszarze **Szczegóły przydziału dysku**. W przypadku obciążeń wybierz z menu rozwijanego preferowany magazyn. Edycja zmienia wartości pozycji **Całkowita ilość miejsca dla magazynu i Wolne miejsce w magazynie** w okienku **Dostępny magazyn dyskowy**. Miejsce poniżej aprowizacji to ilość miejsca, które program DPM sugeruje dodać do woluminu, aby bezproblemowo wykonywać kopie zapasowe w przyszłości.

8. W obszarze **Wybierz metodę tworzenia repliki** określ, jak chcesz obsługiwać początkową pełną replikację danych. W przypadku wybrania replikowania za pośrednictwem sieci zaleca się wybranie czasu w godzinach małego obciążenia sieci. W przypadku dużych ilości danych lub nieoptymalnych warunków sieciowych należy wziąć pod uwagę replikację danych w trybie offline za pomocą nośników wymiennych.

9. W polu **Wybierz opcje sprawdzania spójności** wybierz sposób automatyzacji sprawdzania spójności. Można włączyć uruchamianie sprawdzania tylko wtedy, gdy dane są niespójne, lub zgodnie z harmonogramem. Jeśli nie chcesz konfigurować automatycznego sprawdzania spójności, w dowolnym momencie możesz uruchomić sprawdzanie ręczne, klikając prawym przyciskiem myszy grupę ochrony w obszarze **Ochrona** w konsoli programu DPM i wybierając polecenie **Przeprowadź sprawdzanie spójności**.

10. Jeśli wybrano opcję tworzenia kopii zapasowych w chmurze przy użyciu usługi Azure Backup, sprawdź, czy na stronie **Określanie danych chronionych w trybie online** zaznaczono obciążenia, dla których ma być

tworzona kopia zapasowa na platformie Azure.

11. W obszarze **Określanie harmonogramu tworzenia kopii zapasowych online** określ, jak często mają być wykonywane przyrostowe kopie zapasowe na platformie Azure. Wykonywanie kopii zapasowych można zaplanować na każdy dzień/tydzień/miesiąc/rok, natomiast godziny/daty pozwalają ustalić konkretny czas uruchomienia wykonywania kopii zapasowych. Kopie zapasowe mogą być tworzone maksymalnie dwa razy dziennie. Zawsze podczas wykonywania kopii zapasowej na platformie Azure jest tworzony punkt odzyskiwania danych na podstawie kopii danych przechowywanych w kopii zapasowej na dysku programu DPM.
12. W obszarze **Określ zasady przechowywania danych online** możesz określić sposób przechowywania na platformie Azure punktów odzyskiwania tworzonych na podstawie kopii zapasowych wykonywanych co dzień/tydzień/miesiąc/rok.
13. W obszarze **Wybierz replikację online** określ, jak będzie wykonywana początkowa pełna replikacja danych. Możesz wykonywać replikację za pośrednictwem sieci lub tworzyć kopie zapasowe offline (rozmieszczanie offline). W przypadku kopii zapasowych offline używana jest funkcja Azure Import. Aby uzyskać więcej informacji, zobacz [Przepływ pracy kopii zapasowej offline w usłudze Kopia zapasowa Azure](#).
14. Na stronie **Podsumowanie** przejrzyj ustawienia. Po kliknięciu pozycji **Utwórz grupę** następuje początkowa replikacja danych. Po ukończeniu replikacji grupa ochrony będzie mieć stan **OK** na stronie **Stan**. Następnie odbywa się tworzenie kopii zapasowych zgodnie z ustawieniami grupy ochrony.

Monitorowanie

Po utworzeniu grupy ochrony następuje replikacja początkowa i program DPM rozpoczyna wykonywanie kopii zapasowych i synchronizowanie danych programu SQL Server. Program DPM monitoruje synchronizację początkową i tworzenie kolejnych kopii zapasowych. Możesz monitorować dane programu SQL Server na kilka sposobów:

- Za pomocą domyślnej funkcji monitorowania programu DPM można skonfigurować powiadomienia na potrzeby aktywnego monitorowania (przez publikowanie alertów i konfigurowanie powiadomień). Powiadomienia mogą być przesyłane pocztą e-mail w przypadku alertów krytycznych, ostrzeżeń lub informacji oraz w przypadku informacji o stanie wystąpień procesu odzyskiwania.
- Korzystając z programu Operations Manager, można publikować alerty z poziomu centralnej lokalizacji.

Konfigurowanie powiadomień dotyczących monitorowania

1. W konsoli administratora programu DPM kliknij kolejno pozycje **Monitorowanie** > **Akcja** > **Opcje**.
2. Kliknij pozycję **Serwer SMTP**, a następnie wpisz nazwę serwera, port i adres e-mail, z którego będą wysyłane powiadomienia. Adres musi być prawidłowy.
3. W obszarze **Uwierzytelniony serwer SMTP** wpisz nazwę użytkownika i hasło. Nazwa użytkownika i hasło muszą odpowiadać nazwie konta domeny należącego do osoby, której adres „Od” został opisany w poprzednim kroku. W przeciwnym razie dostarczanie powiadomień nie powiedzie się.
4. Aby przetestować ustawienia serwera SMTP, kliknij pozycję **Wyślij testową wiadomość e-mail**, wpisz adres e-mail, na który serwer programu DPM ma przesłać wiadomość testową, a następnie kliknij przycisk **OK**. Kliknij kolejno pozycje **Opcje** > **Powiadomienia**, a następnie wybierz typy alertów, o których odbiorcy chcą być powiadamiani. W polu **Odbiorcy** wpisz adres e-mail każdego odbiorcy, do którego program DPM ma przysyłać kopie powiadomień.

Konfigurowanie alertów w programie Operations Manager

1. W konsoli administratora programu DPM kliknij kolejno pozycje **Monitorowanie** > **Akcja** > **Opcje** > **Publikowanie alertów** > **Publikuj aktywne alerty**.

2. Po włączeniu opcji **Publikowanie alertów** wszystkie istniejące alerty programu DPM, które mogą wymagać reakcji użytkownika, są publikowane w dzienniku zdarzeń **Alerty programu DPM**. Agent programu Operations Manager, który został zainstalowany na serwerze programu DPM, publikuje te alerty w programie Operations Manager i aktualizuje konsolę w miarę generowania nowych alertów.

Zezwalanie administratorom programu SQL Server na przywracanie danych

Program DPM udostępnia funkcję odzyskiwania samoobsługowego dającą administratorom programu SQL Server dostęp do danych chronionych przez program DPM, co umożliwia przywracanie bazy danych programu SQL Server z kopii zapasowej w folderze sieciowym. Narzędzie programu DPM do odzyskiwania samoobsługowego umożliwia tworzenie ról i zarządzanie nimi, dzięki czemu można określić, którzy użytkownicy mogą wykonywać odzyskiwanie samoobsługowe. Następnie użytkownicy używają Kreatora odzyskiwania samoobsługowego w celu odzyskania baz danych programu SQL Server.

Aby skonfigurować odzyskiwanie samoobsługowe programu SQL Server, wykonaj następujące czynności:

1. W konsoli programu DPM kliknij kolejno pozycje **Ochrona** i **Konfiguruj odzyskiwanie samoobsługowe**.
2. W oknie narzędzia konfiguracji odzyskiwania samoobsługowego programu DPM dla programu SQL Server kliknij pozycję **Utwórz rolę**.
3. Na stronie **grupy zabezpieczeń** utworzysz co najmniej jedną grupę zawierającą użytkowników, dla których chcesz włączyć funkcję odzyskiwania samoobsługowego. Określ grupy zabezpieczeń w formacie domena\grupa zabezpieczeń lub podaj użytkownika w formacie domena\nazwa użytkownika. Do roli programu DPM można dodać wiele grup i użytkowników.
4. Na stronie **Elementy odzyskiwania** określ chronione wystąpienia programu SQL Server oraz bazy danych, dla których chcesz włączyć odzyskiwanie samoobsługowe. Określając wystąpienia, użyj formatu <nazwa komputera\nazwa wystąpienia>. Aby określić bazę danych, naciśnij klawisz TAB, a następnie wpisz nazwę bazy danych. Aby umożliwić użytkownikom ról odzyskanie wszystkich baz danych w wystąpieniu, naciśnij klawisz TAB, a następnie naciśnij klawisz spacji w celu wyczyszczenia tekstu w kolumnie **Nazwa bazy danych**.

Należy pamiętać, że po włączeniu użytkownikom roli programu DPM opcji odzyskiwania wszystkich baz danych programu SQL Server w wystąpieniu programu SQL Server użytkownicy ci mogą także odzyskać dowolne bazy danych programu SQL Server, które zostaną następnie dodane do wystąpienia. Po włączeniu dostępu za pomocą ról programu DPM upewnij się, że wszystkim elementom członkowskim roli przyznano odpowiednie uprawnienia umożliwiające wyświetlanie i uzyskiwanie dostępu do wszystkich baz danych.

5. Aby ograniczyć lokalizacje odzyskiwania dla użytkowników ról, na stronie **Docelowe lokalizacje odzyskiwania** kliknij pozycję **Pozwól użytkownikom na odzyskiwanie baz danych do innego wystąpienia programu SQL Server** i określ co najmniej jedną docelową lokalizację odzyskiwania i ścieżki plików, które są dozwolone. Jeśli chcesz, aby wszystkie ścieżki w wystąpieniu były dozwolone, nie podawaj wartości w polu **Ścieżka odzyskanego pliku**. Po włączeniu tego ustawienia użytkownicy mogą odzyskiwać pliki baz danych przy użyciu dowolnej lokalizacji, dla której mają uprawnienie do zapisu. Użytkownicy nie mogą jednak zastąpić oryginalnych plików bazy danych i jeśli będą podejmować takie próby, Narzędzie do samoobsługowego odzyskiwania programu DPM (SSRT) dla programu SQL Server będzie ich blokować.
6. Ponadto upewnij się, że na komputerze, na którym jest uruchamiane odzyskiwanie samoobsługowe, jest zainstalowana co najmniej wersja 3.5 środowiska .NET Framework oraz Narzędzie do samoobsługowego odzyskiwania programu DPM. Narzędzie to jest dostępne w lokalizacji instalacji produktu DPM, w folderze **DpmSqlEURInstaller**.

Przywracanie danych programu SQL Server

Dane SQL można odzyskać w następujący sposób:

- Odzyskiwanie bazy danych do oryginalnej lokalizacji
- Odzyskiwanie bazy danych o nowej nazwie do jej oryginalnej lokalizacji lub do innego wystąpienia programu SQL Server
- Odzyskiwanie bazy danych do innego wystąpienia programu SQL Server
- Kopiowanie bazy danych do folderu sieciowego
- Kopiowanie bazy danych na taśmę

Należy pamiętać o tym, że nie można odzyskać bazy danych systemu do innego wystąpienia programu SQL Server.

Aby odzyskać bazę danych przy użyciu konsoli programu DPM, wykonaj następujące czynności:

1. W konsoli administratora programu DPM kliknij na pasku nawigacyjnym opcję **Odzyskiwanie**. Korzystając z funkcji przeglądania, wybierz bazę danych do odzyskania.
2. W kalendarzu kliknij dowolną pogrubioną datę, aby pobrać listę punktów odzyskiwania dostępnych dla tej daty. W menu **Godzina odzyskiwania** są wyświetlane godziny poszczególnych dostępnych punktów odzyskiwania. W menu **Godzina odzyskiwania** wybierz punkt odzyskiwania, którego chcesz użyć.
3. W okienku **Akcje** kliknij polecenie **Odzyskaj** uruchomić Kreatora odzyskiwania.
4. Na stronie **Przegląd wybranego elementu do odzyskania** kliknij przycisk **Dalej**. Należy pamiętać o następujących kwestiach:
 - Wybierz lokalizację, do której chcesz odzyskać bazę danych. W przypadku wybrania opcji **Odzyskaj do dowolnego wystąpienia SQL** wprowadź ścieżkę odzyskiwania. Dla odzyskanej bazy danych można określić nową nazwę. Należy pamiętać, że ta opcja jest niedostępna po wybraniu ustawienia **Najnowszy punkt odzyskiwania**.
 - Nie można odzyskać nowszej wersji bazy danych SQL Server do wystąpienia starszej wersji programu SQL Server.
 - Jeśli wybierzesz opcję **Kopiuj do folderu sieciowego**, a wybrany punkt odzyskiwania nie został utworzony przy użyciu funkcji ekspresowej pełnej kopii zapasowej, zostaną wyświetlone nowe opcje punktu odzyskiwania.
 - Jeśli wybierzesz opcję **Kopiuj na taśmę**, a wybrany punkt odzyskiwania nie został utworzony przy użyciu funkcji ekspresowej pełnej kopii zapasowej, zostaną wyświetlone nowe opcje punktu odzyskiwania. W przypadku opcji taśmy należy wybrać bibliotekę taśm, która ma zostać użyta do odzyskiwania.
5. Jeśli został wybrany punkt odzyskiwania inny niż **Najnowszy**, na stronie Określ stan bazy danych wybierz opcję **Pozostaw działającą bazę danych**.
6. Określ opcje odzyskiwania dotyczące ograniczania przepustowości sieci, odzyskiwania wykorzystującego sieć SAN i powiadomień e-mail, a następnie kliknij przycisk **Dalej**.
7. Na stronie **Podsumowanie** przejrzyj ustawienia odzyskiwania, a następnie kliknij przycisk **Odzyskaj**.

Jeśli chcesz przywrócić dane do nie działającej farmy programu SharePoint, musisz utworzyć nową farmę, korzystając z tego samego wystąpienia programu SQL Server i serwera frontonu sieci Web co oryginalna farma. Następnie uruchom następujące polecenie na serwerze frontonu sieci Web używanym przez program DPM do

odzyskiwania danych farmy: `ConfigureSharePoint-EnableSharePointProtection` . Otwórz Kreatora odzyskiwania i w obszarze Dane chronione rozwiń serwer zawierający farmę, którą chcesz odzyskać, a następnie kliknij pozycję **Wszystkie chronione dane farmy**. Wybierz datę i godzinę punktu odzyskiwania, a następnie wybierz opcję odzyskiwania. Pamiętaj o tym, że nie możesz odzyskać całej farmy do innej lokalizacji. Po ukończeniu odzyskiwania na głównym serwerze frontonu sieci Web farmy serwerów uruchom Kreatora konfiguracji programu SharePoint i odłącz serwer frontonu sieci Web od farmy.

Poniższe instrukcje umożliwiają odzyskanie bazy danych użytkownikom z uprawnieniami do odzyskiwania samoobsługowego:

1. Otwórz Narzędzie do samoobsługowego odzyskiwania programu DPM, kliknij pozycję **Połącz z serwerem DPM** i podaj nazwę serwera programu DPM.
2. Po ustanowieniu połączenia kliknij pozycję **Nowe zadanie odzyskiwania**, aby uruchomić Kreatora odzyskiwania.
3. Na stronie kreatora **Określ szczegóły bazy danych** określ wystąpienie programu SQL Server i nazwę bazy danych do odzyskania. Jeśli używasz grup dostępności, użyj formatu **NAZWAGD.NazwaFQDNklastra\NAZWAGD** dla nazwy grupy.
4. Na stronie **Określ punkt odzyskiwania** wybierz datę i godzinę punktu odzyskiwania.
5. Na stronie **Wybierz typ odzyskiwania** wskaż, czy odzyskiwanie ma zostać przeprowadzone przy użyciu dowolnego wystąpienia na tym samym serwerze programu SQL Server czy na innym serwerze. Określ, czy do odzyskiwania ma zostać użyty folder sieciowy. Pamiętaj o tym, że odzyskiwanie do folderu sieciowego jest możliwe tylko w przypadku punktów odzyskiwania utworzonych przy użyciu pełnych ekspresowych kopii zapasowych.
6. W przypadku odzyskiwania do bazy danych na stronie **Określ stan bazy danych** wskaż, czy baza danych ma działać po ukończeniu odzyskiwania i czy chcesz skopiować dzienniki transakcji SQL.
7. Na stronie **Określ opcje odzyskiwania** wskaż, czy chcesz zachować ustawienia zabezpieczeń z serwera źródłowego czy zastosować ustawienia z serwera docelowego. Możesz również wybrać opcję wysłania powiadomienia e-mail po zakończeniu odzyskiwania.

Tworzenie kopii zapasowej komputerów klienckich przy użyciu programu DPM

11.12.2019 • 22 minutes to read

Program System Center Data Protection Manager (DPM) można wdrożyć, aby utworzyć kopię zapasową komputerów klienckich. W zależności od systemu operacyjnego klienta można tworzyć kopie zapasowe woluminów, udziałów, folderów, plików, stanu systemu operacyjnego i woluminu oraz woluminów z deduplikacją.

Wymagania wstępne i ograniczenia

Przed wdrożeniem programu DPM w celu ochrony danych na komputerach klienckich sprawdź wymagania wstępne dotyczące wdrażania:

- Przeczytaj informacje o obsługiwanych systemach operacyjnych klienta w artykule [What can DPM back up?](#) (Co program DPM może umieścić w kopii zapasowej?)
- Przeczytaj [informacje o wersji](#) oraz artykuł [What's supported and what isn't for DPM?](#) (Co jest obsługiwane przez program DPM, a co nie?), który opisuje problemy związane z ochroną klienta.
- Upewnij się, że komputery klienckie, dla których mają być tworzone kopie zapasowe, znajdują się w domenie serwera programu DPM lub w domenie mającej dwukierunkową relację zaufania z domeną programu DPM.
- Aby skonfigurować komputery klienckie do ochrony, należy na nich zainstalować agenta ochrony programu DPM. Jeśli na komputerze klienckim jest skonfigurowana zapor systemu Windows, podczas instalacji agenta zostaną skonfigurowane wymagane wyjątki zapory. W razie konieczności zresetowania zapory można ją ponownie skonfigurować, uruchamiając program SetDpmServer.exe. W przypadku używania innej zapory niż zapor systemu Windows należy otworzyć wymagane porty. Aby dowiedzieć się więcej, zobacz [Deploy the DPM protection agent](#) (Wdrażanie agenta ochrony programu DPM).
- Program DPM może tworzyć kopie zapasowe komputerów klienckich połączonych fizycznie lub bezprzewodowo z siecią lokalną (LAN) lub tworzyć kopie zapasowe za pośrednictwem połączenia VPN. Do tworzenia kopii zapasowych przez połączenia VPN jest wymagane włączenie obsługi protokołu ICMP na komputerze klienckim.
- Każdy serwer DPM może chronić do 3000 komputerów klienckich. W przypadku ochrony komputerów klienckich na dużą skalę firma Microsoft zaleca utworzenie wielu grup ochrony i rozłożenie czasów punktów odzyskiwania dla tych grup ochrony. Im więcej klientów należy do grupy ochrony, tym dłużej zajmuje się wyliczeniem zmian w grupie ochrony.
- Wydajność tworzenia kopii zapasowych danych klienta można dostosować w następujący sposób:
 - Jeśli tworzenie kopii zapasowych danych klienta odbywa się powoli, można ustawić niższą wartość dla następującego klucza: HKLM\Software\Microsoft\Microsoft Data Protection Manager\Agent\ClientProtection\WaitInMSPerRequestForClientRead.
 - Aby zwiększyć wydajność klienta, można dostosować te klucze rejestru:
 - Software\Microsoft\Microsoft Data Protection Manager\Configuration\DPMTaskController\MaxRunningTasksThreshold. Wartość: 9037ebb9-5c1b-4ab8-a446-052b13485f57
 - Software\Microsoft\Microsoft Data Protection

Manager\Configuration\DPMTaskController\MaxRunningTasksThreshold. Wartość:
3d859d8c-d0bb-4142-8696-c0d215203e0d

- Software\Microsoft\Microsoft Data Protection
Manager\Configuration\DPMTaskController\MaxRunningTasksThreshold. Wartość: c4cae2f7-f068-4a37-914e-9f02991868da
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft Data Protection
Manager\Collocation\Client. Wartość: DSCollocationFactor

Przed rozpoczęciem

1. **Wdrażanie programu DPM** — sprawdź, czy program DPM został poprawnie zainstalowany i wdrożony. Jeśli nie zostało to jeszcze zrobione, zobacz:
 - Wymagania systemowe dotyczące programu DPM
 - [Co program DPM może umieścić w kopii zapasowej?](#)
 - [Elementy obsługiwane i nieobsługiwane przez program DPM](#)
 - [Instalowanie programu DPM](#)
2. **Konfigurowanie magazynu** — dane kopii zapasowej można przechowywać na dysku, na taśmie i w chmurze przy użyciu platformy Azure. Więcej informacji znajduje się w temacie [Prepare data storage](#) (Przygotowanie magazynu danych).
3. **Konfigurowanie agenta ochrony DPM** — agent musi być zainstalowany na komputerach klienckich, które mają być chronione. Zapoznaj się z tematem [Deploy the DPM protection agent](#) (Wdrażanie agenta ochrony programu DPM).

Tworzenie kopii zapasowej komputerów klienckich

1. Kliknij kolejno pozycje **Ochrona** > **Akcje** > **Utwórz grupę ochrony**, aby otworzyć kreatora **tworzenia nowej grupy ochrony** w konsoli programu DPM.
2. W obszarze **Wybór grupy ochrony** kliknij opcję **Klienci**. Opcję Klienci należy wybrać tylko wtedy, gdy chcesz utworzyć kopię zapasową danych komputera z wersją kliencką systemu operacyjnego Windows. W przypadku wszystkich innych obciążeń wybierz opcję Serwery. Aby dowiedzieć się więcej, zobacz [Deploy protection groups](#) (Wdrażanie grup ochrony).
3. Na stronie **Wybierz członków grupy** kliknij pozycję **Dodaj wiele komputerów**. Komputery klienckie, dla których chcesz wykonać kopię zapasową, możesz dodać za pomocą pliku tekstowego. Nazwy poszczególnych komputerów muszą znajdować się w osobnych wierszach. Zalecamy wprowadzenie w pełni kwalifikowanych nazw domen komputerów docelowych. Oto przykład wprowadzenia nazw kilku komputerów w pliku txt:
 - K omp1.abc.domain.com
 - K omp2.abc.domain.com
 - K omp3.abc.domain.com

Należy pamiętać, że jeżeli program DPM nie znajdzie pliku tekstowego lub któregoś z komputerów, to doda je do pliku dziennika. Aby otworzyć plik dziennika, kliknij pozycję **Dodanie maszyn nie powiodło się**. Aby dodać nowe komputery klienckie do istniejącej grupy ochrony, kliknij prawym przyciskiem myszy nazwę grupy i wybierz pozycję **Dodaj komputery klienckie**.

- Na stronie **Określ dołączenia i wykluczenia** określ foldery na wybranych komputerach, które mają

być objęte ochroną lub z niej wykluczone. Aby dokonać wyboru z listy dobrze znanych folderów, takich jak **Dokumenty**, kliknij listę rozwijaną. Należy pamiętać o następujących kwestiach:

- Jeśli wykluczysz folder, a następnie określisz oddzielną regułę dołączania dla podfolderu, program DPM nie wykona kopii zapasowej tego podfolderu. Reguła wykluczenia ma pierwszeństwo przed regułą dołączenia.
 - Jeśli dołączysz folder, a następnie określisz oddzielną regułę wykluczenia dla podfolderu, program DPM wykona kopię zapasową całego folderu z wyjątkiem wykluczonego podfolderu.
 - Jeśli dołączysz dobrze znany folder, taki jak **Dokumenty**, program DPM zlokalizuje foldery **Dokumenty** dla wszystkich użytkowników komputera, a następnie zastosuje regułę. Na przykład jeśli profile użytkowników na komputerze **Komp1** zawierają folder **Dokumenty** dla użytkowników Użytkownik1 i Użytkownik2, program DPM wykona kopię zapasową obu folderów.
 - W kolumnie **Folder** wpisz nazwy folderów. Użyj do tego zmiennych, takich jak *programfiles*, lub dokładnych nazw folderów. Wybierz pozycję **Dołącz** lub **Wyklucz** dla każdej pozycji w kolumnie **Reguła**.
 - Zaznaczenie opcji **Zezwalaj użytkownikom na określanie chronionych elementów członkowskich** da użytkownikom końcowym możliwość dodawania na komputerze kolejnych folderów do uwzględniania w kopiach zapasowych. Jednak użytkownicy końcowi nie mogą wybierać plików i folderów, które zostały jawnie wykluczone przez administratora.
 - W obszarze **Wykluczenia typów plików** można za pomocą rozszerzeń plików określić typy plików do wykluczenia.
4. W obszarze **Wybierz metodę ochrony danych** określ, jak mają być obsługiwane krótkoterminowe i długoterminowe kopie zapasowe. Krótkoterminowa kopia zapasowa jest zawsze najpierw tworzona na dysku z opcją przeniesienia kopii zapasowej z dysku do chmury platformy Azure za pomocą usługi Azure Backup (na potrzeby przechowywania krótkoterminowego lub długoterminowego). Zamiast długoterminowej kopii zapasowej w chmurze możesz również skonfigurować długoterminową kopię zapasową na autonomicznym urządzeniu taśmowym lub w bibliotece taśm połączonej z serwerem programu DPM.
5. W polu **Wybierz cele krótkoterminowe** określ sposób tworzenia kopii zapasowej w krótkoterminowym magazynie na dysku. W obszarze Zakres przechowywania określ, jak długo chcesz przechowywać dane na dysku. W obszarze **Częstotliwość synchronizacji** określ, jak często chcesz zapisywać przyrostowe kopie zapasowe na dysku. Jeśli nie chcesz ustawiać interwału kopii zapasowych, możesz zaznaczyć opcję Zaraz przed punktem odzyskiwania, aby program DPM wykonywał ekspresową pełną kopię zapasową bezpośrednio przed każdym zaplanowanym punktem odzyskiwania.
6. Jeśli chcesz utworzyć długoterminową kopię zapasową danych na taśmie, na stronie **Określ cele długoterminowe** wskaż, jak długo chcesz przechowywać dane na taśmie (od 1 roku do 99 lat). W obszarze Częstotliwość wykonywania kopii zapasowych określ, jak często mają być wykonywane kopie zapasowe na taśmie. Częstotliwość zależy od wybranego zakresu przechowywania:
- Gdy zakres przechowywania wynosi 1–99 lat, można wybrać tworzenie kopii zapasowej codziennie, co tydzień, co dwa tygodnie, co miesiąc, co kwartał, co pół roku lub co rok.
 - Gdy zakres przechowywania wynosi 1–11 miesięcy, można wybrać tworzenie kopii zapasowej codziennie, co tydzień, co dwa tygodnie lub co miesiąc.
 - Gdy zakres przechowywania wynosi 1–4 tygodnie, można wybrać tworzenie kopii zapasowej codziennie lub co tydzień.

W przypadku korzystania z autonomicznej stacji taśm dla pojedynczej grupy ochrony program DPM używa

tej samej taśmy do codziennego wykonywania kopii zapasowych do momentu, gdy zabraknie na niej miejsca. Na taśmie można również zapisywać dane z różnych grup ochrony.

Na stronie **Określanie szczegółów taśmy i biblioteki** określ taśmę lub bibliotekę, która ma być używana, oraz czy dane na taśmie mają być kompresowane i szyfrowane.

7. Na stronie **Przejrzyj przydział dysku** przejrzyj miejsce na dysku w puli magazynów przydzielone danej grupie ochrony.

Całkowity rozmiar danych to rozmiar danych, dla których ma zostać utworzona kopia zapasowa, a w obszarze **Miejsce na dysku do udostępnienia w programie DPM** jest widoczna ilość miejsca zalecana przez program DPM dla grupy ochrony. Program DPM wybierze idealną wielkość kopii zapasowej na podstawie ustawień. Opcje wielkości kopii zapasowej można jednak edytować w obszarze **Szczegóły przydziału dysku**. W przypadku obciążeń wybierz z menu rozwijanego preferowany magazyn. Edycja zmienia wartości pozycji **Całkowita ilość miejsca dla magazynu** i **Wolne miejsce w magazynie** w okienku **Dostępny magazyn dyskowy**. Miejsce poniżej aprowizacji to ilość miejsca, które program DPM sugeruje dodać do woluminu, aby bezproblemowo wykonywać kopie zapasowe w przyszłości.

8. W polu **Wybierz metodę tworzenia repliki** określ, jak chcesz obsługiwać początkową pełną replikację danych. W przypadku wybrania replikowania za pośrednictwem sieci zaleca się wybranie czasu w godzinach małego obciążenia sieci. W przypadku dużych ilości danych lub nieoptymalnych warunków sieciowych należy wziąć pod uwagę replikację danych w trybie offline za pomocą nośników wymiennych.
9. W polu **Wybierz opcje sprawdzania spójności** wybierz sposób automatyzacji sprawdzania spójności. Można włączyć uruchamianie sprawdzania tylko wtedy, gdy dane są niespójne, lub zgodnie z harmonogramem. Jeśli nie chcesz konfigurować automatycznego sprawdzania spójności, w dowolnym momencie możesz uruchomić sprawdzanie ręczne, klikając prawym przyciskiem myszy grupę ochrony w obszarze **Ochrona** w konsoli programu DPM i wybierając polecenie **Przeprowadź sprawdzanie spójności**.
10. Jeśli wybrano opcję tworzenia kopii zapasowych w chmurze przy użyciu usługi Azure Backup, sprawdź, czy na stronie **Określanie danych chronionych w trybie online** zaznaczono obciążenia, dla których ma być tworzona kopia zapasowa na platformie Azure.
11. W obszarze **Określanie harmonogramu tworzenia kopii zapasowych online** określ, jak często mają być wykonywane przyrostowe kopie zapasowe na platformie Azure. Wykonywanie kopii zapasowych można zaplanować na każdy dzień/tydzień/miesiąc/rok, natomiast godziny/daty pozwalają ustalić konkretny czas uruchomienia wykonywania kopii zapasowych. Kopie zapasowe mogą być tworzone maksymalnie dwa razy dziennie. Zawsze podczas wykonywania kopii zapasowej na platformie Azure jest tworzony punkt odzyskiwania danych na podstawie kopii danych przechowywanych w kopii zapasowej na dysku programu DPM.
12. W polu **Określ zasady przechowywania danych online** możesz określić sposób przechowywania na platformie Azure punktów odzyskiwania tworzonych na podstawie kopii zapasowych wykonywanych co dzień/tydzień/miesiąc/rok.
13. W polu **Wybierz replikację online** określ, jak będzie wykonywana początkowa pełna replikacja danych. Możesz wykonywać replikację za pośrednictwem sieci lub tworzyć kopie zapasowe offline (rozmieszczanie offline). W przypadku kopii zapasowych offline używana jest funkcja Azure Import. [Przeczytaj więcej](#).
14. Na stronie **Podsumowanie** przejrzyj ustawienia. Po kliknięciu pozycji **Utwórz grupę** następuje początkowa replikacja danych. Po ukończeniu replikacji grupa ochrony będzie mieć stan **OK** na stronie **Stan**. Następnie odbywa się tworzenie kopii zapasowych zgodnie z ustawieniami grupy ochrony.

Odzyskiwanie danych klienta

Za pomocą Kreatora odzyskiwania można odzyskać dane komputera klienckiego. Można również skonfigurować

funkcję odzyskiwania przez użytkownika końcowego, tak aby poszczególni użytkownicy mogli sami odzyskiwać swoje dane.

Zezwolenie klientom na odzyskiwanie swoich danych

Odzyskiwanie przez użytkownika końcowego umożliwia użytkownikom niezależne odzyskiwanie danych plików dzięki pobieraniu punktów odzyskiwania plików. Należy pamiętać o następujących kwestiach:

- Użytkownicy mogą jedynie odzyskać dane przechowywane na dysku.
- Należy zmodyfikować schemat usługi Active Directory w celu umożliwienia działania funkcji odzyskiwania przez użytkownika końcowego. Program DPM rozszerza schemat, tworzy kontener (MS-ShareMapConfiguration), przyznaje uprawnienia serwera programu DPM do zmiany zawartości kontenera i dodaje mapowania między udziałami źródła i repliki. [Zobacz](#) szczegółową listę klas i atrybutów dodanych do usługi AD za pomocą programu DPM.
- W przypadku włączenia odzyskiwania przez użytkownika końcowego nie można określić, na których serwerach plików jest włączona ta funkcja.
- Nie można kontrolować, którzy użytkownicy lub które grupy usługi Active Directory mogą wykonywać odzyskiwanie przez użytkownika końcowego.

Oto czynności, jakie należy wykonać, aby skonfigurować odzyskiwanie przez użytkownika końcowego:

1. Skonfiguruj usługę Active Directory do obsługi odzyskiwania przez użytkownika końcowego:
 - a. W konsoli programu DPM kliknij kolejno pozycje **Opcje > Odzyskiwanie przez użytkownika końcowego > Skonfiguruj usługę Active Directory**.
 - b. W oknie dialogowym **Skonfiguruj usługę Active Directory** wybierz opcję **Użyj bieżących poświadczeń** lub wpisz nazwę użytkownika i hasło do konta, które ma uprawnienia administratora schematu i domeny. Potwierdź ustawienia.
 - c. Jeśli nie masz konta, które ma uprawnienia do planowania i administrowania domeną, możesz polecić innemu użytkownikowi uprawnienia do uruchamiania <dysk:>\Program Files\Microsoft Data Protection Manager\dpm\end User User Recovery\DPMADSchemaExtension.exe na komputerze w tej samej domenie, w której znajduje się serwer DPM. Po uruchomieniu aplikacji użytkownik powinien określić nazwę komputera, na którym chcesz umożliwić odzyskiwanie przez użytkownika końcowego oraz nazwę domeny DNS serwera DPM.

Należy zauważyć, że jeśli chroniony komputer i serwer DPM znajdują się w różnych domenach, schemat musi być rozszerzony za pomocą narzędzia DPMADSchemaExtension.exe uruchomionego w tej drugiej domenie.
2. Po skonfigurowaniu ustawień usługi AD na karcie **Odzyskiwanie przez użytkownika końcowego** kliknij pozycję **Włącz odzyskiwanie przez użytkownika końcowego**.

Odzyskiwanie danych

Aby odzyskać dane przy użyciu konsoli programu DPM, wykonaj następujące czynności:

1. W konsoli programu DPM kliknij na pasku nawigacyjnym opcję **Odzyskiwanie** i wyszukaj dane, które chcesz odzyskać. Wybierz dane w okienku wyników.
2. Dostępne punkty odzyskiwania są zaznaczone w kalendarzu i sekcji punktów odzyskiwania pogrubioną czcionką. Wybierz pogrubioną datę dla punktu odzyskiwania, który chcesz odzyskać.
3. W okienku **Element możliwy do odzyskania** kliknij element, aby wybrać go do odzyskania.
4. W okienku **Akcje** kliknij polecenie **Odzyskaj**. Program DPM uruchomi Kreatora odzyskiwania.

5. Dane można odzyskać w następujący sposób:

- a. **Odzyskaj do oryginalnej lokalizacji.** Należy zauważyć, że to nie zadziała, jeśli komputer kliencki jest połączony za pośrednictwem sieci VPN. W takim przypadku należy użyć alternatywnej lokalizacji, a następnie skopiować dane z tej lokalizacji.
- b. **Odzyskaj do lokalizacji alternatywnej.**
- c. **Kopiuuj na taśmę.** Ta opcja umożliwia kopiowanie woluminu z wybranymi danymi na taśmę w bibliotece programu DPM. Istnieje również możliwość wybrania opcji kompresowania lub szyfrowania danych na taśmie.

6. Określ opcje odzyskiwania:

- a. **Zachowanie funkcji odzyskiwania istniejącej wersji.** Wybierz opcję **Utwórz kopię, Pomiń** lub **Zastąp**. Ta opcja jest dostępna tylko w przypadku odzyskiwania do oryginalnej lokalizacji.
- b. **Przywróć zabezpieczenia.** Wybierz opcję **Zastosuj ustawienia komputera docelowego** lub **Zastosuj ustawienia zabezpieczeń wersji punktu odzyskiwania**.
- c. **Ograniczenie przepustowości.** Kliknij przycisk **Modyfikuj**, aby włączyć ustawienie ograniczenia przepustowości sieci.
- d. **Włącz odzyskiwanie na podstawie SAN z użyciem migawek sprzętowych.** Wybierz tę opcję, aby szybciej odzyskiwać dane przy użyciu migawek sprzętowych opartych na sieci SAN.

Ta opcja przydaje się tylko wtedy, gdy jest włączona funkcja wykonywania migawek sprzętowych z wykorzystaniem sieci SAN, w sieci SAN jest możliwe utworzenie klona, a następnie podzielenie go i skonfigurowanie jako możliwego do zapisu, a komputer chroniony oraz serwer programu DPM są podłączone do tej samej sieci SAN.

- e. **Powiadomienie.** Kliknij opcję **Wyślij wiadomość e-mail po zakończeniu odzyskiwania** i określ adresatów powiadomienia. Kolejne adresy e-mail oddziel przecinkami.

7. Po wybraniu wartości dla wcześniejszych opcji kliknij przycisk **Dalej**.

8. Przejrzyj ustawienia odzyskiwania i kliknij polecenie **Odzyskaj**. Należy zauważyć, że w trakcie odzyskiwania zostaną anulowane wszystkie zadania synchronizacji dla wybranego elementu odzyskiwania.

Użytkownicy końcowi powinni odzyskać dane w następujący sposób:

1. Przejdź do chronionego pliku danych. Kliknij prawym przyciskiem myszy nazwę pliku i wybierz pozycję **Właściwości**.
2. Po kliknięciu kolejno pozycji **Właściwości** > **Poprzednie wersje** wybierz wersję, na podstawie której chcesz przeprowadzić odzyskiwanie.

Tworzenie kopii zapasowej danych plików przy użyciu programu DPM

10.01.2020 • 14 minutes to read

Za pomocą programu System Center Data Protection Manager (DPM) można tworzyć kopie zapasowe danych plików na serwerach i komputerach klienckich.

Przed rozpoczęciem

1. **Wdrażanie programu DPM** — sprawdź, czy program DPM został poprawnie zainstalowany i wdrożony. Zalecamy, aby przejrzeć następujące artykuły:
 - [Wymagania systemowe](#)
 - [Co program DPM może umieścić w kopii zapasowej?](#)
 - [Elementy obsługiwane i nieobsługiwane przez program DPM](#)
 - [Instalowanie programu DPM](#)
2. **Konfigurowanie magazynu** — dane kopii zapasowej można przechowywać na dysku, na taśmie i w chmurze przy użyciu platformy Azure. Więcej informacji znajduje się w temacie [Prepare data storage](#) (Przygotowanie magazynu danych).
3. **Konfigurowanie agenta ochrony programu DPM** — agenta ochrony programu DPM należy zainstalować na każdym komputerze, dla którego mają być tworzone kopie zapasowe. Zapoznaj się z tematem [Deploy the DPM protection agent](#) (Wdrażanie agenta ochrony programu DPM).

Tworzenie kopii zapasowej danych plików

Po skonfigurowaniu infrastruktury programu DPM można włączyć ochronę komputerów, na których znajdują się dane plików, których kopia zapasowa ma być utworzona.

1. W celu utworzenia grupy ochrony kliknij kolejno pozycje **Ochrona** > **Akcje** > **Utwórz grupę ochrony**, aby utworzyć kreatora **tworzenia nowej grupy ochrony** w konsoli programu DPM.
2. Na stronie **Wybierz typ grupy ochrony** wybierz pozycję **Serwery**.
3. Na stronie **Wybierz członków grupy** należy dodać do grupy ochrony maszyny, dla których ma być tworzona kopia zapasowa danych plików. Na tych maszynach wybierz lokalizacje, udziały i foldery, które chcesz chronić. [Wdrażanie grup ochrony](#). Można wybrać różne typy folderów (np. Pulpit) lub różne typy plików. Można również wykluczyć określone lokalizacje z ochrony.
4. W obszarze **Wybierz metodę ochrony danych** określ, jak mają być obsługiwane krótkoterminowe i długoterminowe kopie zapasowe. Krótkoterminowa kopia zapasowa jest zawsze najpierw tworzona na dysku z opcją przeniesienia kopii zapasowej z dysku do chmury platformy Azure za pomocą usługi Azure Backup (na potrzeby przechowywania krótkoterminowego lub długoterminowego). Zamiast długoterminowej kopii zapasowej w chmurze możesz również skonfigurować długoterminową kopię zapasową na autonomicznym urządzeniu taśmowym lub w bibliotece taśm połączonej z serwerem programu DPM.
5. W polu **Wybierz cele krótkoterminowe** określ sposób tworzenia kopii zapasowej w krótkoterminowym magazynie na dysku. W obszarze **Zakres przechowywania** określ, jak długo chcesz przechowywać dane na

dysku. W obszarze **Częstotliwość synchronizacji** określ, jak często chcesz zapisywać przyrostowe kopie zapasowe na dysku. Jeśli nie chcesz ustawiać interwału kopii zapasowych, możesz zaznaczyć opcję **Zaraz** przed punktem odzyskiwania, aby program DPM wykonywał ekspresową pełną kopię zapasową bezpośrednio przed każdym zaplanowanym punktem odzyskiwania.

6. Jeśli chcesz utworzyć długoterminową kopię zapasową danych na taśmie, na stronie **Określ cele długoterminowe** wskaż, jak długo chcesz przechowywać dane na taśmie (od 1 roku do 99 lat). W obszarze **Częstotliwość wykonywania kopii zapasowych** określ, jak często mają być wykonywane kopie zapasowe na taśmie. Częstotliwość zależy od wybranego zakresu przechowywania:

- Gdy zakres przechowywania wynosi 1–99 lat, można wybrać tworzenie kopii zapasowej codziennie, co tydzień, co dwa tygodnie, co miesiąc, co kwartał, co pół roku lub co rok.
- Gdy zakres przechowywania wynosi 1–11 miesięcy, można wybrać tworzenie kopii zapasowej codziennie, co tydzień, co dwa tygodnie lub co miesiąc.
- Gdy zakres przechowywania wynosi 1–4 tygodnie, można wybrać tworzenie kopii zapasowej codziennie lub co tydzień.

W przypadku korzystania z autonomicznej stacji taśm dla pojedynczej grupy ochrony program DPM używa tej samej taśmy do codziennego wykonywania kopii zapasowych do momentu, gdy zabraknie na niej miejsca. Na taśmie możesz również zapisywać dane z różnych grup ochrony.

Na stronie **Określanie szczegółów taśmy i biblioteki** określ taśmę lub bibliotekę, która ma być używana, oraz czy dane na taśmie mają być kompresowane i szyfrowane.

7. Na stronie **Przejrzyj przydział dysku** przejrzyj miejsce na dysku w puli magazynów przydzielone danej grupie ochrony.

Całkowity rozmiar danych to rozmiar danych, dla których ma zostać utworzona kopia zapasowa, a w obszarze **Miejsce na dysku do udostępnienia w programie DPM** jest widoczna ilość miejsca zalecana przez program DPM dla grupy ochrony. Program DPM wybierze idealną wielkość kopii zapasowej na podstawie ustawień. Opcje wielkości kopii zapasowej można jednak edytować w obszarze **Szczegóły przydziału dysku**. W przypadku obciążeń wybierz z menu rozwijanego preferowany magazyn. Edycja zmienia wartości pozycji **Całkowita ilość miejsca dla magazynu** i **Wolne miejsce w magazynie** w okienku **Dostępny magazyn dyskowy**. Miejsce poniżej apro wizacji to ilość miejsca, które program DPM sugeruje dodać do woluminu, aby bezproblemowo wykonywać kopie zapasowe w przyszłości.

8. W polu **Wybierz metodę tworzenia repliki** określ, jak chcesz obsługiwać początkową pełną replikację danych. W przypadku wybrania replikowania za pośrednictwem sieci zaleca się wybranie czasu w godzinach małego obciążenia sieci. W przypadku dużych ilości danych lub nieoptymalnych warunków sieciowych należy wziąć pod uwagę replikację danych w trybie offline za pomocą nośników wymiennych.
9. W polu **Wybierz opcje sprawdzania spójności** wybierz sposób automatyzacji sprawdzania spójności. Można włączyć uruchamianie sprawdzania tylko wtedy, gdy dane są niespójne, lub zgodnie z harmonogramem. Jeśli nie chcesz konfigurować automatycznego sprawdzania spójności, w dowolnym momencie możesz uruchomić sprawdzanie ręczne, klikając prawym przyciskiem myszy grupę ochrony w obszarze **Ochrona** w konsoli programu DPM i wybierając polecenie **Przeprowadź sprawdzanie spójności**.
10. Jeśli wybrano opcję tworzenia kopii zapasowych w chmurze przy użyciu usługi Azure Backup, sprawdź, czy na stronie **Określanie danych chronionych w trybie online** zaznaczono obciążenia, dla których ma być tworzona kopia zapasowa na platformie Azure.
11. W obszarze **Określanie harmonogramu tworzenia kopii zapasowych online** określ, jak często mają być wykonywane przyrostowe kopie zapasowe na platformie Azure. Wykonywanie kopii zapasowych można zaplanować na każdy dzień/tydzień/miesiąc/rok, natomiast godziny/daty pozwalają ustalić konkretny czas

uruchomienia wykonywania kopii zapasowych. Kopie zapasowe mogą być tworzone maksymalnie dwa razy dziennie. Zawsze podczas wykonywania kopii zapasowej na platformie Azure jest tworzony punkt odzyskiwania danych na podstawie kopii danych przechowywanych w kopii zapasowej na dysku programu DPM.

12. W polu **Określ zasady przechowywania danych online** możesz określić sposób przechowywania na platformie Azure punktów odzyskiwania tworzonych na podstawie kopii zapasowych wykonywanych co dzień/tydzień/miesiąc/rok.
13. W polu **Wybierz replikację online** określ, jak będzie wykonywana początkowa pełna replikacja danych. Możesz wykonywać replikację za pośrednictwem sieci lub tworzyć kopie zapasowe offline (rozmieszczanie offline). W przypadku kopii zapasowych offline używana jest funkcja Azure Import. [Przeczytaj więcej](#).
14. Na stronie **Podsumowanie** przejrzyj ustawienia. Po kliknięciu pozycji **Utwórz grupę** następuje początkowa replikacja danych. Po ukończeniu replikacji grupa ochrony będzie mieć stan **OK** na stronie **Stan**. Następnie odbywa się tworzenie kopii zapasowych zgodnie z ustawieniami grupy ochrony.

Odzyskiwanie kopii zapasowej danych plików

Do odzyskiwania danych służy Kreator odzyskiwania. Po dwukrotnym kliknięciu chronionego woluminu w okienku **Chronione dane** w kreatorze program DPM wyświetli w okienku wyników dane znajdujące się na tym woluminie. Nazwy chronionych serwerów można filtrować alfabetycznie, klikając przycisk **Filtruj**. Po wybraniu w widoku drzewa źródła danych do odzyskania można wybrać określony punkt odzyskiwania, klikając w kalendarzu pogrubione daty. W okienku **Akcje** kliknij polecenie **Odzyskaj**. Program DPM uruchomi zadanie odzyskiwania.

Odzyskiwanie danych

Aby odzyskać dane przy użyciu konsoli programu DPM, wykonaj następujące czynności:

1. W konsoli programu DPM kliknij na pasku nawigacyjnym opcję **Odzyskiwanie** i wyszukaj dane, które chcesz odzyskać. Wybierz dane w okienku wyników.
2. Dostępne punkty odzyskiwania są zaznaczone w kalendarzu i sekcji punktów odzyskiwania pogrubioną czcionką. Wybierz pogrubioną datę dla punktu odzyskiwania, który chcesz odzyskać.
3. W okienku **Element możliwy do odzyskania** kliknij element, aby wybrać go do odzyskania.
4. W okienku **Akcje** kliknij polecenie **Odzyskaj**, aby otworzyć Kreatora odzyskiwania.
5. Dane można odzyskać w następujący sposób:
 - a. **Odzyskaj do oryginalnej lokalizacji**. Należy zauważyć, że to nie zadziała, jeśli komputer kliencki jest połączony za pośrednictwem sieci VPN. W takim przypadku należy użyć alternatywnej lokalizacji, a następnie skopiować dane z tej lokalizacji.
 - b. **Odzyskaj do lokalizacji alternatywnej**.
 - c. **Kopiuj na taśmę**. Ta opcja umożliwia skopiowanie woluminu z wybranymi danymi na taśmę w bibliotece programu DPM. Istnieje również możliwość wybrania opcji kompresowania lub szyfrowania danych na taśmie.
6. Określ opcje odzyskiwania:
 - a. **Zachowanie funkcji odzyskiwania istniejącej wersji**. Wybierz opcję **Utwórz kopię**, **Pomiń** lub **Zastąp**. Ta opcja jest dostępna tylko w przypadku odzyskiwania do oryginalnej lokalizacji.
 - b. **Przywróć zabezpieczenia**. Wybierz opcję **Zastosuj ustawienia komputera docelowego** lub **Zastosuj ustawienia zabezpieczeń wersji punktu odzyskiwania**.

c. **Ograniczenie przepustowości.** Kliknij przycisk **Modyfikuj**, aby włączyć ustawienie ograniczenia przepustowości sieci.

d. **Włącz odzyskiwanie na podstawie SAN z użyciem migawek sprzętowych.** Wybierz tę opcję, aby szybciej odzyskiwać dane przy użyciu migawek sprzętowych opartych na sieci SAN.

Ta opcja przydaje się tylko wtedy, gdy jest włączona funkcja wykonywania migawek sprzętowych z wykorzystaniem sieci SAN, w sieci SAN jest możliwe utworzenia klona, a następnie podzielenie go i skonfigurowanie jako możliwego do zapisu, a komputer chroniony oraz serwer programu DPM są podłączone do tej samej sieci SAN.

e. **Powiadomienie.** Kliknij opcję **Wyślij wiadomość e-mail po zakończeniu odzyskiwania** i określ adresatów powiadomienia. Kolejne adresy e-mail oddziel przecinkami.

7. Po wybraniu wartości dla wcześniejszych opcji kliknij przycisk **Dalej**.

8. Przejrzyj ustawienia odzyskiwania i kliknij polecenie **Odzyskaj**. Należy zauważyć, że w trakcie odzyskiwania zostaną anulowane wszystkie zadania synchronizacji dla wybranego elementu odzyskiwania.

W przypadku użycia funkcji Modern Backup Storage funkcja odzyskiwania przez użytkownika końcowego serwera plików nie jest obsługiwana. W przypadku funkcji odzyskiwania przez użytkownika końcowego serwera plików ma miejsce zależność względem usługi kopiowania woluminów w tle (VSS), która nie jest używana przez funkcję Modern Backup Storage. Jeśli odzyskiwanie przez użytkownika końcowego jest włączone, odzyskiwanie danych przebiega w następujący sposób:

1. Przejdź do chronionego pliku danych. Kliknij prawym przyciskiem myszy nazwę pliku i wybierz pozycję **Właściwości**.

2. Po kliknięciu kolejno pozycji **Właściwości** > **Poprzednie wersje** wybierz wersję, którą chcesz odzyskać.

Tworzenie kopii zapasowej stanu systemu i kompletnego stanu systemu

11.12.2019 • 31 minutes to read

Program System Center Data Protection Manager (DPM) może utworzyć kopię zapasową stanu systemu i zapewnić ochronę przed odzyskiwaniem od zera (BMR).

- **Kopia zapasowa stanu systemu:** kopia zapasowa plików systemu operacyjnego, dzięki której możliwe jest odzyskanie stanu systemu, gdy komputer uruchamia się, ale pliki systemowe i rejestr zostały utracone. Kopia zapasowa stanu systemu zawiera:
 - Element członkowski domeny: pliki rozruchowe, baza danych rejestracji klasy COM+, rejestr
 - Kontroler domeny: usługa Active Directory (NTDS), pliki rozruchowe, baza danych rejestracji klasy COM+, rejestr, wolumin systemowy (SYSVOL)
 - Maszyna z uruchomionymi usługami klastrowania: dodatkowa kopia zapasowa metadanych serwera klastra
 - Maszyna z uruchomionymi usługami certyfikatów: dodatkowa kopia zapasowa danych certyfikatu
- **Kopia zapasowa kompletnego stanu systemu:** tworzona jest kopia zapasowa plików systemu operacyjnego i wszystkich danych z wyjątkiem danych użytkownika na woluminach krytycznych. Zgodnie z definicją kopia zapasowa BMR obejmuje kopię zapasową stanu systemu. Zapewnia ochronę, gdy maszyna nie zostanie uruchomiona i konieczne będzie odzyskanie wszystkiego.

Ta tabela podsumowuje elementy, których kopię zapasową można wykonać i które można odzyskać. Szczegółowe informacje o wersjach aplikacji, które mogą być chronione przy użyciu kopii zapasowej stanu systemu i BMR, znajdziesz w temacie [Co program DPM może umieścić w kopii zapasowej?](#)

KOPIA ZAPASOWA	PROBLEM	ODZYSKIWANIE Z KOPII ZAPASOWEJ PROGRAMU DPM	ODZYSKIWANIE Z KOPII ZAPASOWEJ STANU SYSTEMU	BMR
Dane pliku Regularne tworzenie kopii zapasowej danych Kopia zapasowa stanu systemu/kompletnego o stanu systemu	Utracone dane pliku	T	N	N
Dane pliku Kopia zapasowa programu DPM danych pliku Kopia zapasowa stanu systemu/kompletnego o stanu systemu	Utracony/uszkodzony system operacyjny	N	T	T

KOPIA ZAPASOWA	PROBLEM	ODZYSKIWANIE Z KOPII ZAPASOWEJ PROGRAMU DPM	ODZYSKIWANE Z KOPII ZAPASOWEJ STANU SYSTEMU	BMR
Dane pliku Kopia zapasowa programu DPM danych pliku Kopia zapasowa stanu systemu/kompletnego o stanu systemu	Utracony serwer (nieuszkodzone woluminy danych)	N	N	T
Dane pliku Kopia zapasowa programu DPM danych pliku Kopia zapasowa stanu systemu/kompletnego o stanu systemu	Utracony serwer (utracone woluminy danych)	T	Nie	Tak (Odzyskiwanie BMR, po którym następuje zwykłe odzyskiwanie kopii zapasowej danych plików)
Dane programu SharePoint: Kopia zapasowa programu DPM danych farmy Kopia zapasowa stanu systemu/kompletnego o stanu systemu	Utracona witryna, listy, elementy listy, dokumenty	T	N	N
Dane programu SharePoint: Kopia zapasowa programu DPM danych farmy Kopia zapasowa stanu systemu/kompletnego o stanu systemu	Uszkodzony lub utracony system operacyjny	N	T	T
Dane programu SharePoint: Kopia zapasowa programu DPM danych farmy Kopia zapasowa stanu systemu/kompletnego o stanu systemu	Odzyskiwanie po awarii	N	N	N

KOPIA ZAPASOWA	PROBLEM	ODZYSKIWANIE Z KOPII ZAPASOWEJ PROGRAMU DPM	ODZYSKIWANIE Z KOPII ZAPASOWEJ STANU SYSTEMU	BMR
Funkcja Hyper-V Kopia zapasowa programu DPM hosta lub gościa funkcji Hyper-V Kopia zapasowa stanu systemu/kompletnego o stanu systemu hosta	Utracona maszyna wirtualna	T	N	N
Funkcja Hyper-V Kopia zapasowa programu DPM hosta lub gościa funkcji Hyper-V Kopia zapasowa stanu systemu/kompletnego o stanu systemu hosta	Uszkodzony lub utracony system operacyjny	N	T	T
Funkcja Hyper-V Kopia zapasowa programu DPM hosta lub gościa funkcji Hyper-V Kopia zapasowa stanu systemu/kompletnego o stanu systemu hosta	Utracony host funkcji Hyper-V (nieuszkodzone maszyny wirtualne)	N	N	T
Funkcja Hyper-V Kopia zapasowa programu DPM hosta lub gościa funkcji Hyper-V Kopia zapasowa stanu systemu/kompletnego o stanu systemu hosta	Utracony host funkcji Hyper-V (utracone maszyny wirtualne)	N	N	T Odzyskiwanie BMR, po którym następuje zwykłe odzyskiwanie programu DPM
Program SQL Server/Exchange Kopia zapasowa aplikacji programu DPM Kopia zapasowa stanu systemu/kompletnego o stanu systemu	Utracone dane aplikacji	T	N	N

KOPIA ZAPASOWA	PROBLEM	ODZYSKIWANIE Z KOPII ZAPASOWEJ PROGRAMU DPM	ODZYSKIWANIE Z KOPII ZAPASOWEJ STANU SYSTEMU	BMR
Program SQL Server/Exchange Kopia zapasowa aplikacji programu DPM Kopia zapasowa stanu systemu/kompletnego o stanu systemu	Uszkodzony lub utracony system operacyjny	N	t	T
Program SQL Server/Exchange Kopia zapasowa aplikacji programu DPM Kopia zapasowa stanu systemu/kompletnego o stanu systemu	Utracony serwer (nieuszkodzone dzienniki transakcji i baz danych)	N	N	T
Program SQL Server/Exchange Kopia zapasowa aplikacji programu DPM Kopia zapasowa stanu systemu/kompletnego o stanu systemu	Utracony serwer (utracone dzienniki transakcji i baz danych)	N	N	T Odzyskiwanie BMR, po którym następuje zwykłe odzyskiwanie programu DPM

Jak działa tworzenie kopii zapasowej stanu systemu

- Po uruchomieniu kopii zapasowej stanu systemu program DPM komunikuje się z usługą WSB w celu utworzenia kopii zapasowej stanu systemu serwera. Domyślnie program DPM i usługa WSB będą używały dysku z największą ilością wolnego miejsca, a informacje dotyczące tego dysku są zapisywane w pliku PSDataSourceConfig.XML. Na tym dysku usługa WSB będzie również wykonywała kopie zapasowe.
- Można wybrać dysk, który będzie używany przez program DPM do tworzenia kopii zapasowej stanu systemu. Aby to zrobić na serwerze chronionym, przejdź do *dysku*: \Program Files\Microsoft Data Protection Manager\DPM\Datasources. Otwórz plik PSDataSourceConfig.XML do edycji. Zmień wartość <FilesToProtect> na literę dysku. Zapisz i zamknij plik. Jeśli grupa ochrony chroni stan systemu komputera, należy uruchomić sprawdzanie spójności. Jeśli sprawdzenie spójności spowoduje wygenerowanie alertu, kliknij link **Modyfikuj grupę ochrony** w alercie, a następnie postępuj zgodnie z krokami kreatora. Po zakończeniu uruchom inne sprawdzanie spójności.
- Należy zwrócić uwagę, że jeśli serwer ochrony znajduje się w klastrze, może się zdarzyć, że dysk klastra zostanie wybrany jako dysk z największą ilością wolnego miejsca. Jest to ważne, ponieważ w przypadku przekazania własności dysku do innego węzła i uruchomienia tworzenia kopii zapasowej stanu systemu ten dysk nie będzie dostępny i wykonywanie kopii zapasowej zakończy się niepowodzeniem. W takim przypadku należy zmodyfikować plik PSDataSourceConfig.XML tak, aby wskazywał dysk lokalny.
- Kopia zapasowa systemu Windows Server (WSB) tworzy folder o nazwie WindowsImageBackup w katalogu

głównym. Podczas tworzenia kopii zapasowej wszystkie dane są umieszczane w tym folderze. Po zakończeniu wykonywania kopii zapasowej plik zostanie przesłany na serwer DPM. Należy pamiętać o następujących kwestiach:

- Ten folder i jego zawartość nie są czyszczone po wykonaniu kopii zapasowej lub zakończeniu transferu. Najlepiej jest przyjąć, że to miejsce pozostaje zarezerwowane dla następnej kopii zapasowej.
- Ten folder jest tworzony przy każdym tworzeniu kopii zapasowej. Sygnatura czasowa wskazuje godzinę wykonania ostatniej kopii zapasowej stanu systemu.

Wykonywanie kopii zapasowej BMR

1. W przypadku kopii zapasowych BMR (w tym kopii zapasowej stanu systemu) zadanie utworzenia kopii zapasowej jest wykonywane bezpośrednio w udziale serwera DPM, a nie w folderze na serwerze chronionym.
2. Serwer DPM wywołuje usługę WSB i udostępnia wolumin repliki dla kopii zapasowej BMR. W takim przypadku program nie nakazuje usłudze WSB skorzystania z dysku z największą ilością wolnego miejsca, ale zaleca użycie udziału utworzonego dla zadania.
3. Po zakończeniu tworzenia kopii zapasowej plik jest przekazywany do serwera programu DPM. Dzienniki są przechowywane w folderze C:\Windows\Logs\WindowsServerBackup.

Wymagania wstępne i ograniczenia

- Odzyskiwanie BMR nie jest obsługiwane na komputerach z systemem Windows Server 2003 ani na komputerach z klienckimi systemami operacyjnymi.
- Nie można używać jednocześnie ochrony BMR i stanu systemu dla komputera znajdującego się w różnych grupach ochrony.
- Serwer programu DPM nie może chronić siebie samego przy pomocy metody BMR.
- Krótkoterminowa ochrona na taśmie (D2T) nie jest obsługiwana w scenariuszach BMR. Długoterminowa ochrona na taśmie (D2D2T) jest obsługiwana.
- Funkcja Kopia zapasowa systemu Windows Server musi być zainstalowana na komputerze chronionym w scenariuszu BMR.
- W przypadku ochrony BMR (w przeciwieństwie do ochrony stanu systemu) program DPM nie ma żadnych wymagań dotyczących miejsca na komputerze chronionym. Usługa Kopia zapasowa systemu Windows Server (WSB) przesyła kopie zapasowe bezpośrednio na serwer DPM. Należy zauważyć, że to zadanie nie jest wyświetlane w widoku zadań programu DPM.
- Jeśli używasz Nowoczesny magazyn kopii zapasowych i chcesz zwiększyć domyślny rozmiar repliki BMR > 30 GB, użyj klucza rejestru: HKLM\Software\Microsoft\Microsoft Data Protection Manager\Configuration ReplicaSizeInGBForSystemProtectionWithBMR (DWORD).
- Jeśli używasz Nowoczesny magazyn kopii zapasowych, SystemState i BMR kopie zapasowe zużywają więcej magazynu (niż starszy magazyn) z powodu klonowania plików ReFS. Każda kopia zapasowa SystemState lub BMR to pełny punkt odzyskiwania. Aby wyeliminować to użycie magazynu, warto:
 - Zaplanuj mniej stanu systemu lub BMR punktów odzyskiwania,
 - Użyj mniejszego okresu przechowywania dla punktów odzyskiwania,
 - Zwiększ dostępny magazyn dla kopii zapasowych stanu systemu lub BMR.

NOTE

Następujące ograniczenia nie mają zastosowania do Nowoczesny magazyn kopii zapasowych (MB). Poniższe ograniczenia mają zastosowanie tylko w przypadku korzystania ze starszej wersji magazynu, po uaktualnieniu programu DPM 2012 R2 do programu DPM 2016.

- Program DPM rezerwuje 30 GB miejsca na woluminie repliki na potrzeby kopii zapasowej BMR. Tę wartość można zmienić na stronie Alokacja dysku w Kreatorze modyfikacji grup ochrony lub za pomocą polecenia cmdlet Get-DatasourceDiskAllocation i Set-DatasourceDiskAllocation w programie PowerShell. Na woluminie punktu odzyskiwania ochrona BMR wymaga około 6 GB do przechowywania danych przez pięć dni. Należy zauważyć, że nie można zmniejszyć rozmiaru woluminu repliki do wartości mniejszej niż 15 GB. Program DPM nie oblicza rozmiaru źródła danych BMR, ale przyjmuje wartość 30 GB dla wszystkich serwerów. Administratorzy powinni zmienić tę wartość w zależności od rozmiaru kopii zapasowych BMR oczekiwanego w swoich środowiskach. Rozmiar kopii zapasowej BMR może być w przybliżeniu obliczony jako suma miejsca używanego przez wszystkie woluminy krytyczne: woluminy krytyczne = wolumin rozruchowy + wolumin systemowy + wolumin obsługujący dane o stanie systemu, takie jak dane usługi AD. Proces tworzenia kopii zapasowej stanu systemu
- W przypadku przełączenia z ochrony stanu systemu na ochronę BMR ochrona BMR będzie wymagać mniej miejsca w **woluminie punktu odzyskiwania**. Dodatkowe miejsce w woluminie nie zostanie jednak odzyskane. Rozmiar woluminu można zmniejszyć ręcznie na strony **Modyfikacja alokacji dysku Kreatora modyfikacji grupy ochrony** lub za pomocą poleceń cmdlet Get-DatasourceDiskAllocation i Set-DatasourceDiskAllocation.

W przypadku przełączenia z ochrony stanu systemu na ochronę BMR ochrona BMR będzie wymagać więcej miejsca w **woluminie repliki**. Wolumin zostanie rozszerzony automatycznie. Jeśli chcesz zmienić domyślne alokacje miejsca, możesz użyć polecenia Modify-DiskAllocation.

- Po przełączeniu z ochrony BMR na ochronę stanu systemu potrzeba będzie więcej miejsca w woluminie punktu odzyskiwania. Program DPM może podjąć próbę automatycznego zwiększenia woluminu. Jeśli w puli magazynów jest za mało miejsca, zostanie wygenerowany błąd.

Po przełączeniu z ochrony BMR na ochronę stanu systemu potrzebne będzie miejsce na komputerze chronionym, ponieważ ochrona stanu systemu najpierw zapisuje replikę na komputerze lokalnym, a następnie przekazuje ją do serwera programu DPM

Przed rozpoczęciem

1. **Wdrażanie programu DPM:** Sprawdź poprawność wdrożenia programu DPM. Jeśli nie zostało to jeszcze zrobione, zobacz:
 - Wymagania systemowe dotyczące programu DPM
 - [Co program DPM może umieścić w kopii zapasowej?](#)
 - [Elementy obsługiwane i nieobsługiwane przez program DPM](#)
 - [Instalowanie programu DPM](#)
2. **Konfigurowanie magazynu** — dane kopii zapasowej można przechowywać na dysku, na taśmie i w chmurze przy użyciu platformy Azure. Więcej informacji znajduje się w temacie [Prepare data storage](#) (Przygotowanie magazynu danych).
3. **Konfigurowanie agenta ochrony programu DPM** — agenta ochrony programu DPM należy zainstalować na komputerze, dla którego ma być utworzona kopia zapasowa. Zapoznaj się z tematem

Tworzenie kopii zapasowej stanu systemu i kompletnego stanu systemu

Konfigurowanie grupy ochrony zgodnie z opisem w temacie [Deploy protection groups](#) (Wdrażanie grup ochrony). Należy zauważyć, że nie można chronić funkcji BMR i stanu systemu na tym samym komputerze w różnych grupach oraz że po wybraniu funkcji BMR stan systemu jest automatycznie włączany.

1. Kliknij kolejno pozycje **Ochrona > Akcje > Utwórz grupę ochrony**, aby otworzyć kreatora **tworzenia nowej grupy ochrony** w konsoli programu DPM.

2. W obszarze **Wybór grupy ochrony** kliknij opcję **Serwery**.

3. W polu **Wybierz członków grupy** rozwiń maszynę i wybierz pozycję **BMR** lub **stan systemu**

Należy pamiętać, że nie można chronić funkcji BMR i stanu systemu na tym samym komputerze w różnych grupach oraz że po wybraniu funkcji BMR stan systemu jest automatycznie włączany. Aby dowiedzieć się więcej, zobacz [Deploy protection groups](#) (Wdrażanie grup ochrony).

4. W obszarze **Wybierz metodę ochrony danych** określ, jak mają być obsługiwane krótkoterminowe i długoterminowe kopie zapasowe. Krótkoterminowe kopie zapasowe zawsze są na dysku, z opcją tworzenia kopii zapasowej na dysku w chmurze platformy Azure przy użyciu usługi Azure Backup (na krótko lub długoterminowe). Zamiast długoterminowej kopii zapasowej w chmurze możesz również skonfigurować długoterminową kopię zapasową na autonomicznym urządzeniu taśmowym lub w bibliotece taśm połączonej z serwerem programu DPM.

5. W polu **Wybierz cele krótkoterminowe** określ sposób tworzenia kopii zapasowej w krótkoterminowym magazynie na dysku. W obszarze Zakres przechowywania określ, jak długo chcesz przechowywać dane na dysku. W obszarze Częstotliwość synchronizacji określ, jak często chcesz zapisywać przyrostowe kopie zapasowe na dysku. Jeśli nie chcesz ustawiać interwału kopii zapasowych, możesz sprawdzić, tuż przed punktem odzyskiwania, aby program DPM wykonał ekspresową pełną kopię zapasową tuż przed zaplanowaniem każdego punktu odzyskiwania.

6. Jeśli chcesz utworzyć długoterminową kopię zapasową danych na taśmie, na stronie **Określ cele długoterminowe** wskaż, jak długo chcesz przechowywać dane na taśmie (od 1 roku do 99 lat). W obszarze Częstotliwość wykonywania kopii zapasowych określ, jak często mają być wykonywane kopie zapasowe na taśmie. Częstotliwość zależy od wybranego zakresu przechowywania:

- Gdy zakres przechowywania wynosi 1–99 lat, można wybrać tworzenie kopii zapasowej codziennie, co tydzień, co dwa tygodnie, co miesiąc, co kwartał, co pół roku lub co rok.
- Gdy zakres przechowywania wynosi 1–11 miesięcy, można wybrać tworzenie kopii zapasowej codziennie, co tydzień, co dwa tygodnie lub co miesiąc.
- Gdy zakres przechowywania wynosi 1–4 tygodnie, można wybrać tworzenie kopii zapasowej codziennie lub co tydzień.

W przypadku korzystania z autonomicznej stacji taśm dla pojedynczej grupy ochrony program DPM używa tej samej taśmy do codziennego wykonywania kopii zapasowych do momentu, gdy zabraknie na niej miejsca. Na taśmie można również zapisywać dane z różnych grup ochrony.

Na stronie **Określanie szczegółów taśmy i biblioteki** określ taśmę lub bibliotekę, która ma być używana, oraz czy dane na taśmie mają być kompresowane i szyfrowane.

7. Na stronie **Przejrzyj przydział dysku** przejrzyj miejsce na dysku w puli magazynów przydzielone danej grupie ochrony.

Całkowity rozmiar danych to rozmiar danych, dla których ma zostać utworzona kopia zapasowa, a w

obszarze **Miejsce na dysku do udostępnienia w programie DPM** jest widoczna ilość miejsca zalecana przez program DPM dla grupy ochrony. Program DPM wybierze idealną wielkość kopii zapasowej na podstawie ustawień. Opcje wielkości kopii zapasowej można jednak edytować w obszarze **Szczegóły przydziału dysku**. W przypadku obciążeń wybierz z menu rozwijanego preferowany magazyn. Edycja zmienia wartości pozycji **Całkowita ilość miejsca dla magazynu i Wolne miejsce w magazynie** w okienku **Dostępny magazyn dyskowy**. Miejsce poniżej apro wizacji to ilość miejsca, które program DPM sugeruje dodać do woluminu, aby bezproblemowo wykonywać kopie zapasowe w przyszłości.

8. W polu **Wybierz metodę tworzenia repliki** określ, jak chcesz obsługiwać początkową pełną replikację danych. W przypadku wybrania replikowania za pośrednictwem sieci zaleca się wybranie czasu w godzinach małego obciążenia sieci. W przypadku dużych ilości danych lub nieoptymalnych warunków sieciowych należy wziąć pod uwagę replikację danych w trybie offline za pomocą nośników wymiennych.
9. W polu **Wybierz opcje sprawdzania spójności** wybierz sposób automatyzacji sprawdzania spójności. Można włączyć uruchamianie sprawdzania tylko wtedy, gdy dane są niespójne, lub zgodnie z harmonogramem. Jeśli nie chcesz konfigurować automatycznego sprawdzania spójności, w dowolnym momencie możesz uruchomić sprawdzanie ręczne, klikając prawym przyciskiem myszy grupę ochrony w obszarze **Ochrona** w konsoli programu DPM i wybierając polecenie **Przeprowadź sprawdzanie spójności**.
10. Jeśli wybrano opcję tworzenia kopii zapasowych w chmurze przy użyciu usługi Azure Backup, sprawdź, czy na stronie **Określanie danych chronionych w trybie online** zaznaczono obciążenia, dla których ma być tworzona kopia zapasowa na platformie Azure.
11. W obszarze **Określanie harmonogramu tworzenia kopii zapasowych online** określ, jak często mają być wykonywane przyrostowe kopie zapasowe na platformie Azure. Wykonywanie kopii zapasowych można zaplanować na każdy dzień/tydzień/miesiąc/rok, natomiast godziny/daty pozwalają ustalić konkretny czas uruchomienia wykonywania kopii zapasowych. Kopie zapasowe mogą być tworzone maksymalnie dwa razy dziennie. Za każdym razem, gdy wykonywana jest kopia zapasowa, na platformie Azure jest tworzony punkt odzyskiwania danych z kopii kopii zapasowej danych przechowywanych na dysku programu DPM.
12. W polu **Określ zasady przechowywania danych online** możesz określić sposób przechowywania na platformie Azure punktów odzyskiwania tworzonych na podstawie kopii zapasowych wykonywanych co dzień/tydzień/miesiąc/rok.
13. W polu **Wybierz replikację online** określ, jak będzie wykonywana początkowa pełna replikacja danych. Możesz wykonywać replikację za pośrednictwem sieci lub tworzyć kopie zapasowe offline (rozmieszczanie offline). W przypadku kopii zapasowych offline używana jest funkcja Azure Import. [Przeczytaj więcej](#).
14. Na stronie **Podsumowanie** przejrzyj ustawienia. Po kliknięciu pozycji **Utwórz grupę** następuje początkowa replikacja danych. Po ukończeniu replikacji grupa ochrony będzie mieć stan **OK** na stronie **Stan**. Następnie odbywa się tworzenie kopii zapasowych zgodnie z ustawieniami grupy ochrony.

Odzyskiwanie stanu systemu lub odzyskiwanie systemu od zera (BMR)

Możliwe jest odzyskanie systemu od zera (BMR) lub odzyskanie stanu systemu w lokalizacji sieciowej. Jeśli utworzono kopię zapasową BMR, użyj środowiska odzyskiwania systemu Windows (WinRE) do uruchomienia systemu i połączenia się z siecią. Użyj narzędzia Kopia zapasowa systemu Windows Server, aby odzyskać informacje z lokalizacji sieciowej. Jeśli wykonano kopię zapasową stanu systemu, wystarczy użyć narzędzia Kopia zapasowa systemu Windows Server w celu odzyskania informacji z lokalizacji sieciowej.

Przywracanie systemu od zera (BMR)

Uruchamianie odzyskiwania na serwerze DPM:

1. W okienku Odzyskiwanie wyszukaj komputer, którego odzyskiwanie chcesz przeprowadzić, i wybierz polecenie Odzyskiwanie systemu od zera.

2. Dostępne punkty odzyskiwania są pogrubione w kalendarzu. Wybierz datę i godzinę dla punktu odzyskiwania, którego chcesz użyć.
3. Na stronie **Wybierz typ odzyskiwania** wybierz pozycję **Kopiuj do folderu sieciowego**.
4. Na stronie **Określ miejsce docelowe** wybierz miejsce, do którego chcesz skopiować dane. Należy pamiętać, że w wybranym miejscu musi być wystarczająco dużo miejsca. Zalecane jest utworzenie nowego folderu.
5. Na stronie **Określ opcje odzyskiwania** wybierz ustawienia zabezpieczeń do zastosowania i wybierz, czy chcesz użyć migawek sprzętowych opartych na sieci SAN, aby szybciej odzyskiwać dane (opcja dostępna tylko wtedy, gdy masz sieć SAN z włączoną tą funkcją oraz możliwością tworzenia i dzielenia klonu w celu umożliwienia zapisu. Ponadto chroniony komputer i serwer programu DPM muszą być podłączone do tej samej sieci).
6. Ustaw opcje powiadamiania i kliknij pozycję **Odzyskiwanie** na stronie **Podsumowanie**.

Konfigurowanie lokalizacji udziału:

1. W lokalizacji przywracania przejdź do folderu zawierającego kopię zapasową.
2. Udostępnij folder znajdujący się powyżej folderu WindowsImageBackup, tak aby katalogiem głównym folderu udostępnionego był folder WindowsImageBackup. W przeciwnym razie przywracanie nie odnajdzie kopii zapasowej. Aby nawiązać połączenie przy użyciu środowiska WinRE, potrzebny jest udział, do którego można uzyskać dostęp ze środowiska WinRE z poprawnym adresem IP i poświadczeniami.

Przywracanie systemu:

1. Uruchom komputer, którego obraz chcesz przywrócić, używając dysku DVD odzyskiwanego systemu Windows.
2. Na pierwszym ekranie sprawdź ustawienia języka/ustawienia regionalne. Na ekranie **Instalacja** wybierz opcję **Napraw komputer**.
3. Na stronie **Opcje odzyskiwania systemu** wybierz kolejno opcje **Przywróć komputer przy użyciu utworzonego wcześniej obrazu systemu**
4. Na stronie **Wybierz kopię zapasową obrazu systemu** wybierz kolejno opcje **Wybierz obraz systemu > Zaawansowane > Wyszukaj obraz systemu w sieci**. Jeśli zostanie wyświetlone ostrzeżenie, wybierz opcję **Tak**. Przejdź do ścieżki udziału, wprowadź poświadczenia i wybierz punkt odzyskiwania. Spowoduje to uruchomienie skanowania w poszukiwaniu określonych kopii zapasowych, które są dostępne dla tego punktu odzyskiwania. Wybierz punkt odzyskiwania.
5. W polu **Wybierz sposób przywracania kopii zapasowej** wybierz opcję **Formatuj dyski i ponownie podziel na partycje**. W następnym oknie sprawdź ustawienia, a następnie kliknij przycisk **Zakończ** w celu rozpoczęcia przywracania. Jeśli to konieczne, uruchom ponownie system.

Przywracanie stanu systemu

Uruchamianie odzyskiwania na serwerze DPM:

1. W okienku Odzyskiwanie wyszukaj komputer, którego odzyskiwanie chcesz przeprowadzić, i wybierz polecenie Odzyskiwanie systemu od zera.
2. Dostępne punkty odzyskiwania są pogrubione w kalendarzu. Wybierz datę i godzinę dla punktu odzyskiwania, którego chcesz użyć.
3. Na stronie **Wybierz typ odzyskiwania** wybierz pozycję **Kopiuj do folderu sieciowego**.
4. Na stronie **Określ miejsce docelowe** wybierz miejsce, do którego chcesz skopiować dane. Należy

pamiętać, że w wybranym miejscu musi być wystarczająco dużo miejsca. Zalecane jest utworzenie nowego folderu.

5. Na stronie **Określ opcje odzyskiwania** wybierz ustawienia zabezpieczeń do zastosowania i wybierz, czy chcesz użyć migawek sprzętowych opartych na sieci SAN, aby szybciej odzyskiwać dane (opcja dostępna tylko wtedy, gdy masz sieć SAN z włączoną tą funkcją oraz możliwością tworzenia i dzielenia klonu w celu umożliwienia zapisu. Ponadto chroniony komputer i serwer programu DPM muszą być podłączone do tej samej sieci).
6. Ustaw opcje powiadamiania i kliknij pozycję **Odzyskiwanie** na stronie **Podsumowanie**.

Uruchamianie programu Kopia zapasowa systemu Windows Server

1. Kliknij pozycję **Akcje > Odzyskaj > Ten serwer > Dalej**.
2. Kliknij pozycję **Inny serwer > strona Określanie typu lokalizacji > Zdalny folder udostępniony**. Podaj ścieżkę do folderu, który zawiera punkt odzyskiwania.
3. Na stronie **Wybierz typ odzyskiwania** kliknij pozycję **Stan systemu**. Na stronie **Wybieranie lokalizacji dla odzyskiwania stanu systemu** kliknij pozycję **Lokalizacja oryginalna**.
4. Na stronie **Potwierdzenie** kliknij pozycję **Odzyskaj**. Po przywróceniu będzie konieczne ponowne uruchomienie serwera.
5. Przywracanie stanu systemu można również uruchomić z wiersza polecenia. Aby to zrobić, uruchom program Kopia zapasowa systemu Windows Server na komputerze, który chcesz odzyskać. W wierszu polecenia wpisz polecenie: **wbadmin get versions -backuptarget <servername\sharename>** , aby uzyskać identyfikator wersji.

Użyj identyfikatora wersji, aby uruchomić przywracanie stanu systemu. W wierszu polecenia wpisz:

Wbadmin start systemstaterecovery-Version:<podanawersja>-backupTarget: <servername\sharename > potwierdzić, że chcesz rozpocząć odzyskiwanie. Możesz śledzić proces w oknie wiersza polecenia. Tworzony jest dziennik przywracania. Po przywróceniu będzie konieczne ponowne uruchomienie serwera.

Tworzenie kopii zapasowych i przywracanie maszyn wirtualnych VMware za pomocą programu DPM

14.02.2020 • 55 minutes to read

W tym artykule wyjaśniono, jak używać programu Data Protection Manager (DPM) w wersji 1801 lub nowszej, aby utworzyć kopię zapasową maszyn wirtualnych działających w systemie 5,5, 6,0, 6,5 lub 6,7 w wersjach oprogramowania VMware vCenter i vSphere funkcji hypervisor (ESXi).

Obsługiwane funkcje oprogramowania VMware

Program DPM 1801 i nowsze oferują następujące funkcje podczas tworzenia kopii zapasowych maszyn wirtualnych VMware:

NOTE

Tworzenie kopii zapasowej na taśmie jest obsługiwane przez program DPM 2019.

- Tworzenie kopii zapasowej bez agenta: program DPM nie wymaga zainstalowania agenta na serwerze vCenter lub ESXi, aby utworzyć kopię zapasową maszyny wirtualnej. Zamiast tego wystarczy podać adres IP lub w pełni kwalifikowaną nazwę domeny (FQDN) oraz poświadczenia logowania używane do uwierzytelniania serwera VMware za pomocą programu DPM.
- Zintegrowana kopia zapasowa w chmurze: program DPM chroni obciążenia na dysku, na taśmie i w chmurze. Przepływ pracy tworzenia kopii zapasowych i odzyskiwania w programie DPM ułatwia zarządzanie długoterminowym przechowywaniem i zapasami poza siedzibą firmy.
- Wykrywanie i ochrona maszyn wirtualnych zarządzanych przez serwer vCenter: program DPM wykrywa i chroni maszyny wirtualne wdrożone na serwerze VMware (serwer vCenter lub ESXi). W miarę wzrostu rozmiaru wdrożenia Użyj programu vCenter do zarządzania środowiskiem programu VMware. Program DPM wykrywa także maszyny wirtualne zarządzane przez program vCenter, co pozwala chronić duże wdrożenia.
- Funkcja autoochrony na poziomie folderów: program vCenter umożliwia organizowanie maszyn wirtualnych w folderach maszyn wirtualnych. Program DPM wykrywa te foldery i umożliwia ochronę maszyn wirtualnych na poziomie folderu i zawiera wszystkie podfoldery. W przypadku ochrony folderów program DPM nie tylko chroni maszyny wirtualne w tym folderze, ale również chroni maszyny wirtualne dodane później. Program DPM wykrywa codziennie nowe maszyny wirtualne i chroni je automatycznie. Podczas organizowania maszyn wirtualnych w folderach cyklicznych program DPM automatycznie wykrywa i chroni nowe maszyny wirtualne wdrożone w folderach cyklicznych.
- Program DPM chroni maszyny wirtualne przechowywane na dysku lokalnym, w systemie plików NFS lub w magazynie klastra.
- Program DPM chroni maszyny wirtualne migrowane pod kątem równoważenia obciążenia: maszyny wirtualne są migrowane pod kątem równoważenia obciążenia, program DPM automatycznie wykrywa i kontynuuje ochronę maszyny wirtualnej.
- Program DPM może odzyskiwać pliki/foldery z maszyny wirtualnej z systemem Windows bez odzyskiwania całej maszyny wirtualnej, co ułatwia szybkie odzyskiwanie potrzebnych plików.

Wymagania wstępne i ograniczenia

Przed rozpoczęciem tworzenia kopii zapasowej maszyny wirtualnej VMware zapoznaj się z poniższą listą

ograniczeń i wymagań wstępnych.

- Jeśli używasz programu DPM do ochrony serwera VMware jako systemu Windows Server, nie możesz użyć tej samej w pełni kwalifikowanej nazwy domeny (FQDN) ani statycznego adresu IP. Jeśli używasz nazwy FQDN do identyfikowania maszyny wirtualnej VMware, użyj statycznego adresu IP do identyfikowania serwera VMware. Jeśli używasz statycznego adresu IP do identyfikowania maszyny wirtualnej VMware wcześniej, użyj nazwy FQDN, aby zidentyfikować maszynę wirtualną VMware. Nie można użyć dynamicznego adresu IP. Należy zauważyć, że agenta programu DPM nie należy wypchnąć do systemu Windows Server działającego jako VMware vCenter Server.
- Jeśli używasz programu vCenter do zarządzania serwerami ESXi w środowisku, Dodaj program vCenter (a nie ESXi) do grupy ochrony programu DPM.
- Program DPM nie może chronić maszyn wirtualnych VMware na pomocniczym serwerze programu DPM.
- Nie można utworzyć kopii zapasowej migawek użytkownika przed pierwszą kopią zapasową programu DPM. Po zakończeniu tworzenia pierwszej kopii zapasowej przez program DPM można utworzyć kopię zapasową migawek użytkownika.
- Program DPM nie może chronić maszyn wirtualnych VMware z dyskami przekazującymi i fizycznymi mapowaniami urządzeń nieprzetworzonych (pRDM).
- Program DPM nie może wykryć ani chronić programu VMware oprogramowania vApps.
- Program DPM nie może chronić maszyn wirtualnych VMware przy użyciu istniejących migawek.

Konfigurowanie programu DPM do ochrony oprogramowania VMware

Poniżej znajdują się szczegółowe informacje dotyczące konfigurowania programu VMware do ochrony w programie DPM. Aby nawiązać komunikację między programem DPM a serwerem VMware, należy skonfigurować poświadczenia programu VMware i nawiązać bezpieczne połączenie między programem DPM a serwerem VMware vCenter Server lub VMware vSphere funkcji hypervisor (ESXi). Jeśli używasz obu vCenter Server i serwera ESXi, skonfiguruj tylko vCenter Server do pracy z programem DPM. Nie musisz dodawać serwerów ESXi do programu DPM. Aby zarządzać serwerem VMware, program DPM potrzebuje prawidłowych poświadczeń w celu uzyskania dostępu do serwerów VMware.

Zarządzanie poświadczeniami

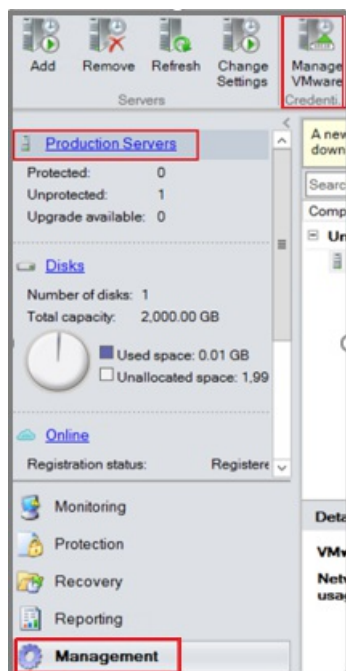
Program DPM nie używa agenta do komunikowania się z serwerem VMware. Zamiast tego program DPM używa poświadczeń nazwy użytkownika i hasła do uwierzytelniania komunikacji zdalnej z serwerem VMware. Za każdym razem, gdy program DPM komunikuje się z serwerem VMware, należy uwierzytelnić program DPM. Ponieważ może być konieczna zmiana poświadczeń, a centrum danych może mieć wiele serwerów vCenter wymagających unikatowych poświadczeń, śledzenie tych poświadczeń może stanowić problem. Program DPM ma jednak funkcję zarządzania poświadczeniami VMware w celu bezpiecznego przechowywania poświadczeń i zarządzania nimi.

Zwróć uwagę na następujące informacje dotyczące poświadczeń:

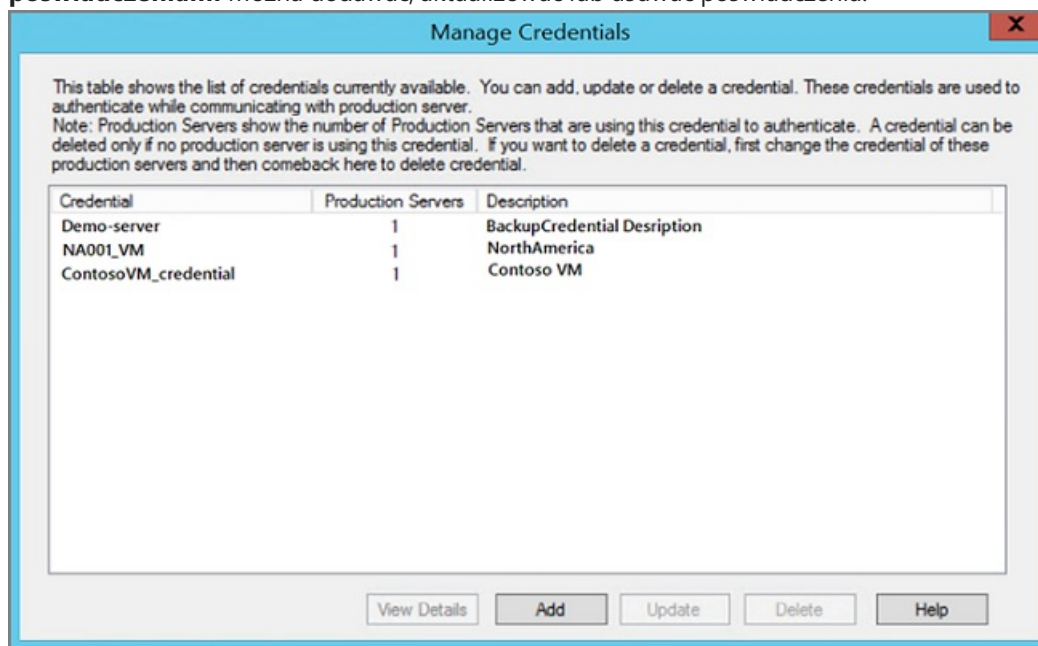
- Jedno poświadczenie może służyć do uwierzytelniania wielu serwerów VMware.
- Gdy zostaną zaktualizowane szczegóły poświadczeń, takie jak opis, nazwa użytkownika i hasło, program DPM użyje tych poświadczeń do komunikowania się ze wszystkimi serwerami VMware.
- Poświadczenia można usunąć tylko wtedy, gdy nie jest on używany do uwierzytelniania serwera VMware.

Otwórz funkcję Zarządzaj poświadczeniami programu VMware

1. W Konsola administratora programu DPM kliknij pozycję **Zarządzanie**.



2. Na liście zasobów do zarządzania kliknij pozycję **serwery produkcyjne**.
3. Na Wstążce narzędzi kliknij polecenie **Zarządzaj poświadczeniami programu VMware**. Zostanie otwarte okno dialogowe **Zarządzanie poświadczeniami**. Za pomocą okna dialogowego **Zarządzanie poświadczeniami** można dodawać, aktualizować lub usuwać poświadczenia.



Zobacz następujące sekcje, aby uzyskać szczegółowe informacje na temat dodawania, aktualizowania lub usuwania poświadczeń.

Dodaj poświadczenia serwera VMware

Należy dodać poświadczenia do serwera programu DPM, aby można było je sparować z poświadczeniami na serwerze VMware. Pamiętaj, że poświadczenia na serwerze programu DPM muszą być takie same jak poświadczenia na serwerze VMware. Aby dodać poświadczenie, w oknie dialogowym **Zarządzanie poświadczeniami**:

1. Kliknij przycisk **Dodaj**, aby otworzyć okno dialogowe Dodawanie poświadczeń.

2. Wpisz informacje w polach **Nazwa**, **Opis**, **Nazwa użytkownika** i **hasło** . Po dodaniu tekstu w wymaganych polach przycisk **Dodaj** zostanie uaktywniony.
 - **Nazwa** jest wyświetlana w kolumnie **poświadczenia** okna dialogowego Zarządzanie poświadczeniami. **Nazwa** jest polem wymaganym i jest identyfikatorem poświadczeń. Nie można edytować tego pola później. Jeśli chcesz zmienić nazwę poświadczenia, musisz dodać nowe poświadczenie.
 - **Opis to tekst opisujący** lub alternatywna nazwa, aby można było rozpoznać lub odróżnić poświadczenia w oknie dialogowym Zarządzanie poświadczeniami. Tekst **opisu** jest polem opcjonalnym i pojawia się w kolumnie **Opis** okna dialogowego Zarządzanie poświadczeniami.
 - **Nazwa użytkownika** i **hasło** to nazwa użytkownika i hasło dla konta użytkownika używanego do uzyskiwania dostępu do serwera. Oba pola są wymagane.
3. Kliknij przycisk **Dodaj** , aby zapisać nowe poświadczenia. Po utworzeniu poświadczeń można użyć ich do uwierzytelniania za pomocą serwera VMware.

Aktualizowanie poświadczeń serwera VMware

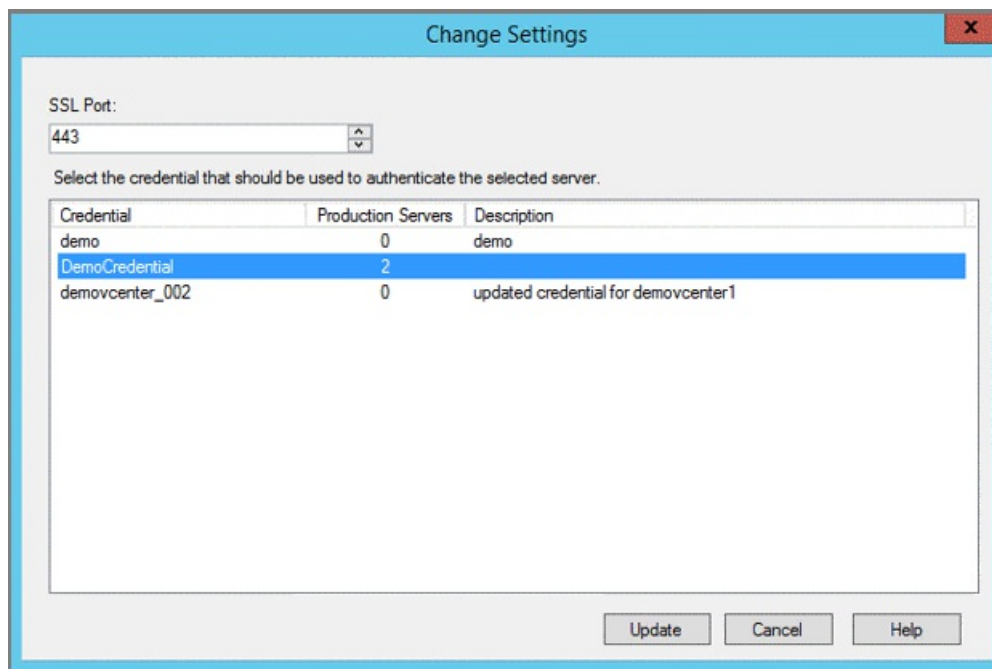
Większość organizacji musi zaktualizować poświadczenia ze względów bezpieczeństwa lub zmian personelu. Po zmianie poświadczeń serwera VMware należy również zaktualizować poświadczenia używane przez program DPM. Jeśli zostały zmienione poświadczenia serwera VMware (nazwa użytkownika i hasło), należy dodać pasujące poświadczenia w programie DPM.

Po dopasowaniu poświadczeń w programie DPM zaktualizuj poświadczenia serwera VMware, wykonując następujące czynności:

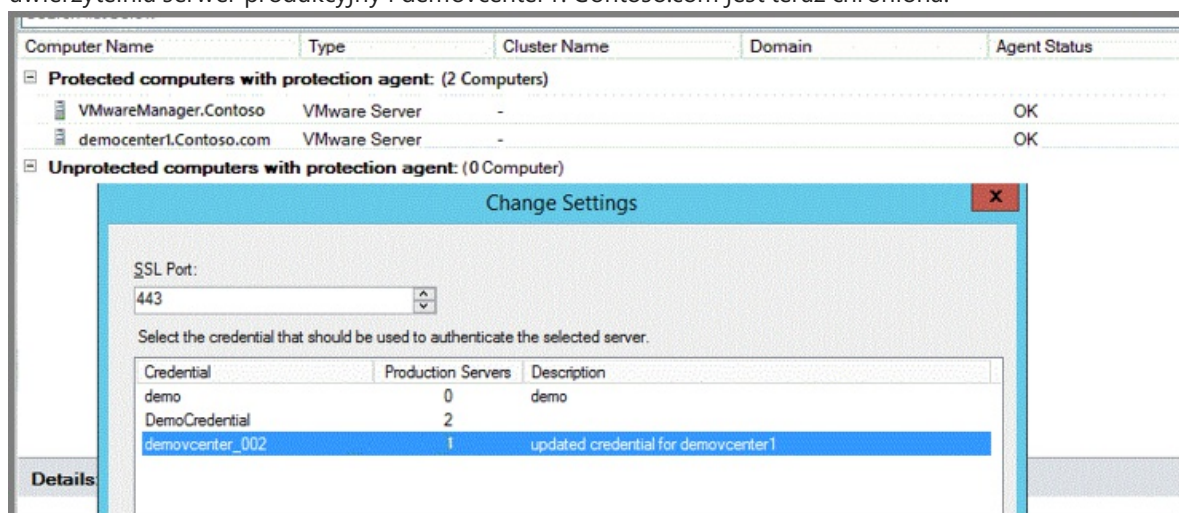
1. W konsoli administratora programu DPM kliknij pozycję **Zarządzanie**.
2. Na liście zasobów do zarządzania kliknij pozycję **serwery produkcyjne**.
3. Na liście komputerów wybierz serwer VMware, którego poświadczenia wymagają aktualizacji. W przykładowym obrazie *demovcenter1*. *Contoso.com* jest serwerem VMware z uszkodzonymi poświadczeniami.

Computer Name	Type	Cluster Name	Domain	Agent Status
Protected computers with protection agent: (1 Computer)				
VMwareManager.Contoso	VMware Server	-		OK
Unprotected computers with protection agent: (1 Computer)				
demovcenter1.Contoso.com	VMware Server	-		Error

4. Na Wstążce narzędzia konsoli administratora kliknij przycisk **Zmień ustawienia**. Zostanie otwarte okno dialogowe zmiana ustawień. Wyświetla wszystkie poświadczenia na serwerze DPM. Na przykładowym obrazie, *demovcenter_002* jest poświadczenia programu DPM do sparowania z *demovcenter1*. *Contoso.com*.



5. Z listy wybierz poświadczenia na serwerze programu DPM, aby dopasować je do poświadczeń programu VMware, a następnie kliknij przycisk **Aktualizuj**. Na obrazie Zwróć uwagę, demovcenter_002 uwierzytelnia serwer produkcyjny i demovcenter1. Contoso.com jest teraz chroniona.



Usuń poświadczenia serwera VMware

Usunięcie poświadczeń powoduje usunięcie poświadczeń z listy na serwerze DPM. Program DPM nie zezwala na usuwanie poświadczeń, które są używane do uwierzytelniania serwera produkcyjnego.

Aby usunąć poświadczenie

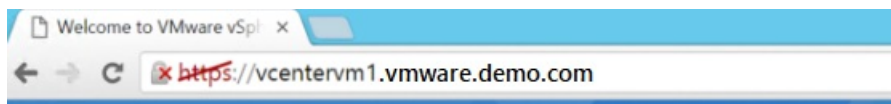
1. W Konsola administratora programu DPM kliknij pozycję Zarządzanie, kliknij pozycję Serwery produkcyjne, a następnie na Wstążce narzędzi kliknij pozycję Zarządzaj poświadczeniami programu VMware.
2. W oknie dialogowym Zarządzanie poświadczeniami wybierz poświadczenie. Upewnij się, że poświadczenie nie jest skojarzone z żadnym serwerem produkcyjnym.
3. Kliknij przycisk **Usuń**, aby usunąć poświadczenie z listy.

Konfigurowanie bezpiecznej komunikacji między programem DPM a serwerem VMware

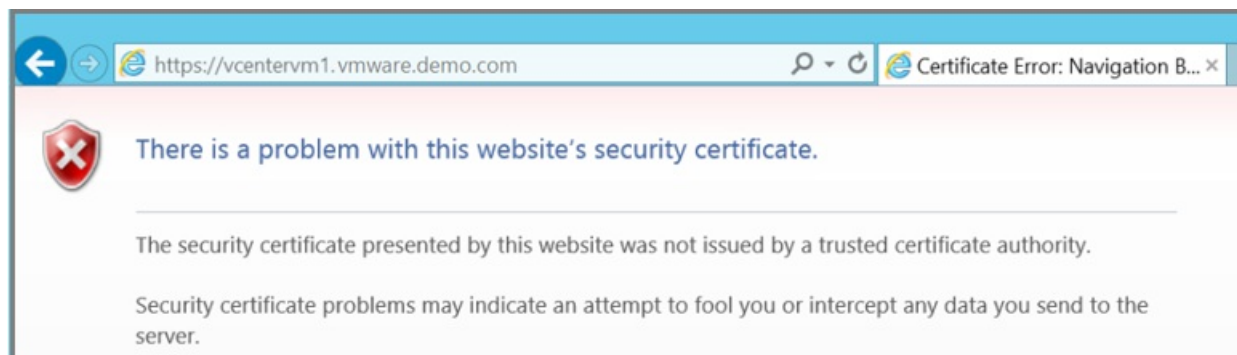
Program DPM komunikuje się z serwerem VMware bezpiecznie za pośrednictwem kanału HTTPS. Aby utworzyć bezpieczną komunikację, zainstaluj zaufany certyfikat na serwerze VMware i serwerze DPM. Jeśli połączenie z programem vCenter nie jest bezpieczne, można je zabezpieczyć, instalując certyfikat na serwerze DPM. Użyj tego samego certyfikatu, aby nawiązać bezpieczne połączenie z serwerem VMware.

Aby sprawdzić, czy istnieje bezpieczny kanał komunikacji między programami DPM i vCenter, Otwórz

przeglądarkę na serwerze programu DPM i uzyskaj dostęp do serwera VMware. Jeśli używasz programu Chrome i nie masz prawidłowego certyfikatu, zobaczysz przekreślony adres URL, taki jak w poniższym przykładzie:



Jeśli używasz programu Internet Explorer i nie masz ważnego certyfikatu, zobaczysz ten komunikat podczas uzyskiwania dostępu do adresu URL:

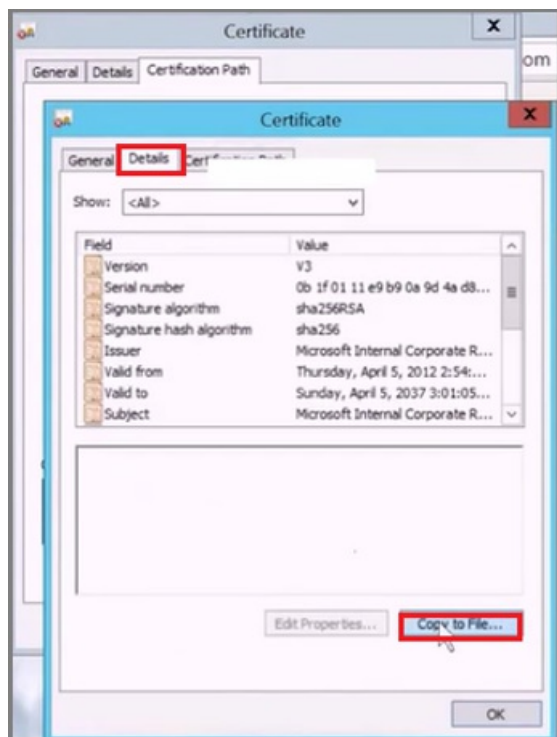


Aby naprawić ten błąd, zainstaluj prawidłowy certyfikat na serwerze DPM i serwerze VMware. W poprzednich obrazach serwer DPM ma prawidłowy certyfikat, ale certyfikat nie znajduje się w magazynie zaufanych głównych urzędów certyfikacji. Aby rozwiązać ten problem, Dodaj certyfikat do serwera VMware.

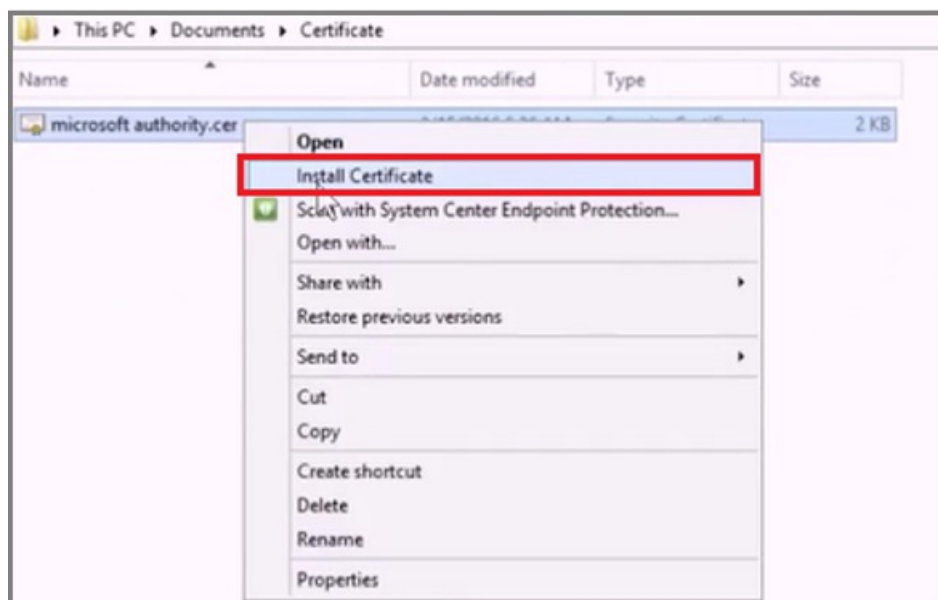
1. W oknie dialogowym certyfikat na karcie **Ścieżka certyfikacji** kliknij przycisk **Wyświetl certyfikat**.



2. W oknie dialogowym Nowy certyfikat kliknij kartę **szczegóły**, a następnie kliknij przycisk **Kopiuj do pliku**, aby otworzyć Kreatora eksportu certyfikatów.



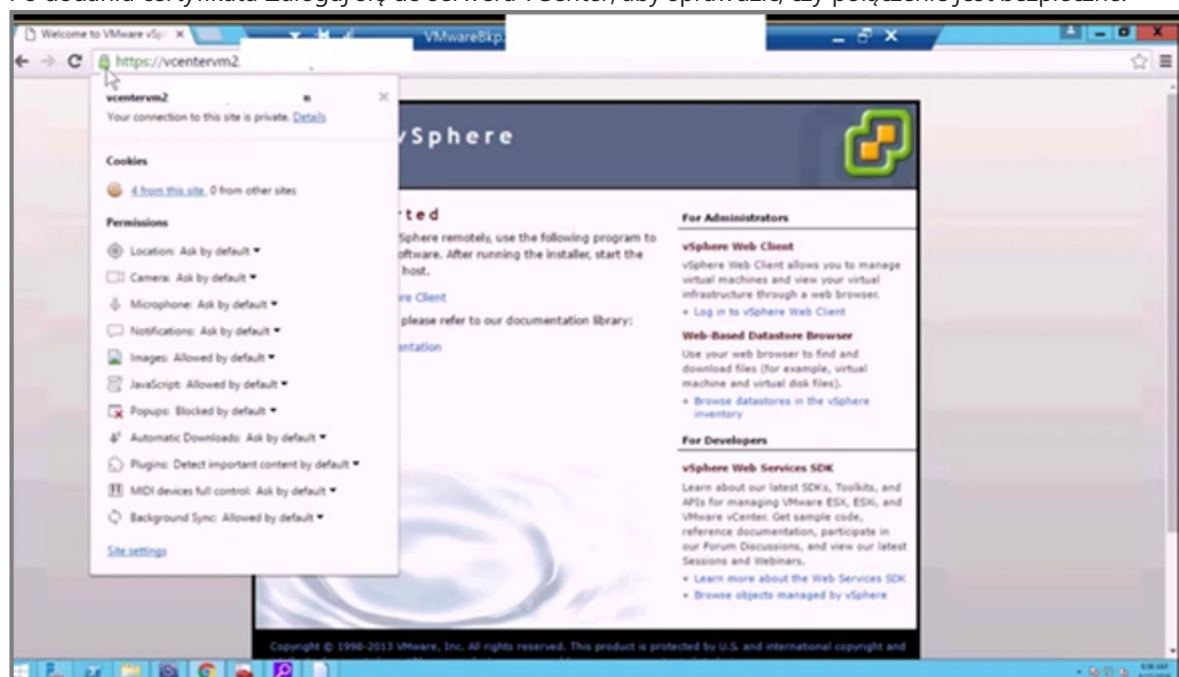
3. W **Kreatorze eksportu certyfikatów** kliknij przycisk **dalej**, a na ekranie **Format pliku eksportu** wybierz pozycję **der encoded binary X. 509 (. CER)**, a następnie kliknij przycisk **dalej**.
4. Na ekranie **plik do wyeksportowania** wpisz nazwę certyfikatu, a następnie kliknij przycisk **dalej**.
5. Kliknij przycisk **Zakończ**, aby zakończyć pracę **Kreatora eksportu certyfikatów**.
6. Znajdź wyeksportowany certyfikat. Kliknij prawym przyciskiem myszy certyfikat, a następnie wybierz polecenie **Zainstaluj certyfikat**, aby otworzyć **Kreatora importu certyfikatów**.



7. W **Kreatorze importu certyfikatów** kliknij przycisk **komputer lokalny**, a następnie kliknij przycisk **dalej**.
8. Aby znaleźć lokalizację, w której chcesz umieścić certyfikat, na ekranie **magazynu certyfikatów**, kliknij pozycję **Umieść wszystkie certyfikaty w następującym magazynie** i kliknij przycisk **Przeglądaj**.
9. W oknie dialogowym **Wybieranie magazynu certyfikatów** wybierz pozycję **zaufany certyfikat głównego urzędu certyfikacji**, a następnie kliknij przycisk **OK**.



10. Kliknij przycisk **dalej**, a następnie kliknij przycisk **Zakończ**, aby zaimportować certyfikat pomyślnie.
11. Po dodaniu certyfikatu Zaloguj się do serwera vCenter, aby sprawdzić, czy połączenie jest bezpieczne.



Dodaj nowe konto użytkownika na serwerze VMware

Program DPM używa nazwy użytkownika i hasła jako poświadczeń do komunikacji i uwierzytelniania za pomocą serwera VMware. Konto użytkownika vCenter ma co najmniej następujące uprawnienia, które są wymagane do pomyślnej ochrony maszyny wirtualnej.

W poniższej tabeli przedstawiono uprawnienia, które należy przypisać do tworzonego konta użytkownika:

UPRAWNIENIA DLA PROGRAMU VCENTER 6,5 I NOWSZEGO KONTA UŻYTKOWNIKA	UPRAWNIENIA DLA KONTA UŻYTKOWNIKA VCENTER 6,0	UPRAWNIENIA DLA KONTA UŻYTKOWNIKA VCENTER 5,5
Magazyn danych. AllocateSpace		
Magazyn danych. Przeglądaj magazyn danych	Magazyn danych. AllocateSpace	Network. Assign
Magazyn danych. operacje na plikach niskiego poziomu	Global. Zarządzaj atrybutami niestandardowymi	Magazyn danych. AllocateSpace
Klaster magazynu danych. Konfigurowanie klastra magazynu danych	Global. Set — atrybut niestandardowy	VirtualMachine.Config.ChangeTracking

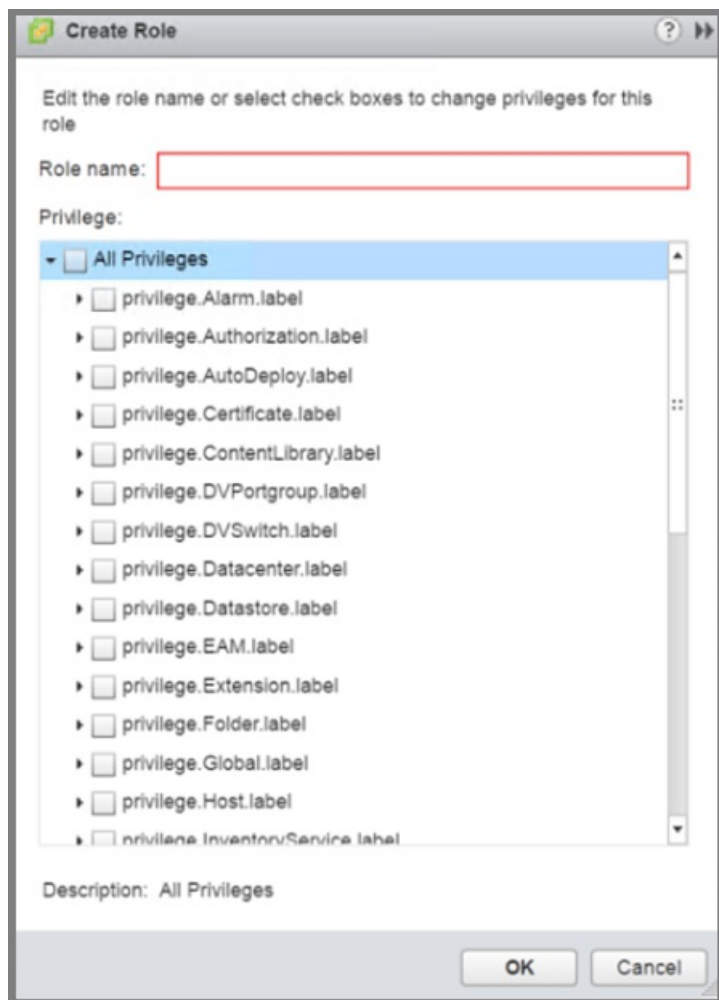
UPRAWNIENIA DLA PROGRAMU VCENTER 6,5 I NOWSZEGO KONTA UŻYTKOWNIKA	UPRAWNIENIA DLA KONTA UŻYTKOWNIKA VCENTER 6,0	UPRAWNIENIA DLA KONTA UŻYTKOWNIKA VCENTER 5,5
Global. Disable, metody	Operacje hosta. local. Utwórz maszynę wirtualną	VirtualMachine.State.RemoveSnapshot
Global. Enable — metody	NFS. Przypisywanie sieci	VirtualMachine.State.CreateSnapshot
Globalne. licencje	Zasoby. Przypisz maszynę wirtualną do puli zasobów	VirtualMachine.Provisioning.DiskRandomRead
Zdarzenie globalne. log	Maszyna wirtualna. Konfiguracja. Dodaj nowy dysk	VirtualMachine.Interact.PowerOff
Global. Zarządzaj atrybutami niestandardowymi	Maszyna wirtualna. Konfiguracja. Advanced	VirtualMachine.Inventory.Create
Global. Set — atrybut niestandardowy	Maszyna wirtualna. Konfiguracja. śledzenie zmian dysku	VirtualMachine.Config.AddNewDisk
Sieć. Przypisywanie sieci	Maszyna wirtualna. Konfiguracja. host USB Device	VirtualMachine.Config.HostUSBDevice
Zasoby. Przypisz maszynę wirtualną do puli zasobów	Maszyna wirtualna. Configuration. Query — pliki nienależące	VirtualMachine.Config.AdvancedConfig
Maszyna wirtualna. Konfiguracja. Dodaj nowy dysk	Maszyna wirtualna. Swapfile	VirtualMachine.config.SwapPlacement
Maszyna wirtualna. Konfiguracja. Advanced	Maszyna wirtualna. Interakcja. Zasilanie wyłączone	Global.ManageCustomFields
Maszyna wirtualna. Konfiguracja. śledzenie zmian dysku	Maszyna wirtualna. Towar. Utwórz nowy	
Maszyna wirtualna. Konfiguracja. dzierżawa dysku	Maszyna wirtualna. Inicjowanie obsługi administracyjnej. Zezwalaj na dostęp do dysku	
Maszyna wirtualna. Konfiguracja. zwiększanie dysku wirtualnego	Maszyna wirtualna. Apropozycji. Zezwalaj na dostęp do dysku tylko do odczytu	
Maszyna wirtualna. Operacje gościa. modyfikacje operacji gościa	Maszyna wirtualna. Zarządzanie migawkami. Utwórz migawkę	
Maszyna wirtualna. Operacje gościa. wykonywanie programu operacji gościa	Maszyna wirtualna. Zarządzanie migawkami. Usuń migawkę	
Maszyna wirtualna. Operacje gościa. zapytania dotyczące operacji gościa		
Maszyna wirtualna. Udziału. Połączenie z urządzeniem		

UPRAWNIENIA DLA PROGRAMU VCENTER 6,5 I NOWSZEGO KONTA UŻYTKOWNIKA	UPRAWNIENIA DLA KONTA UŻYTKOWNIKA VCENTER 6,0	UPRAWNIENIA DLA KONTA UŻYTKOWNIKA VCENTER 5,5
Maszyna wirtualna. Udziału. Zarządzanie systemem operacyjnym gościa za pomocą interfejsu API VIX		
Maszyna wirtualna. Spis. Rejestr		
Maszyna wirtualna. Spis. Remove		
Maszyna wirtualna. Inicjowanie obsługi administracyjnej. Zezwalaj na dostęp do dysku		
Maszyna wirtualna. Inicjowanie obsługi administracyjnej. Zezwalaj na dostęp do dysku tylko do odczytu		
Maszyna wirtualna. Inicjowanie obsługi administracyjnej. Zezwalaj na pobieranie maszyny wirtualnej		
Maszyna wirtualna. Zarządzanie migawkami. Utwórz migawkę		
Maszyna wirtualna. Zarządzanie migawkami. Usuń migawkę		
Maszyna wirtualna. Zarządzanie migawkami. Przywróć migawkę		
vApp. Dodaj maszynę wirtualną		
vApp. Przypisz pulę zasobów		
vApp. Unregister		

Zalecane kroki do przypisywania tych uprawnień:

Utwórz rolę, na przykład BackupAdminRole

1. W programie vSphere Web Client z menu **Nawigator** kliknij pozycję **Administracja > role**.
2. Z menu rozwijanego **dostawca ról** wybierz vCenter Server, do którego zostanie zastosowana rola.
3. W okienku **role** kliknij przycisk "+", aby otworzyć okno dialogowe **Tworzenie roli** i utworzyć rolę.



4. Nazwij rolę, **BackupAdminRole**.
5. Wybierz uprawnienia (określone na poprzedniej liście punktowanej) dla roli i kliknij przycisk **OK**.

Utwórz nowego użytkownika, na przykład BackupAdmin

Podczas tworzenia użytkownika ten użytkownik musi znajdować się w tej samej domenie co obiekty, które mają być chronione.

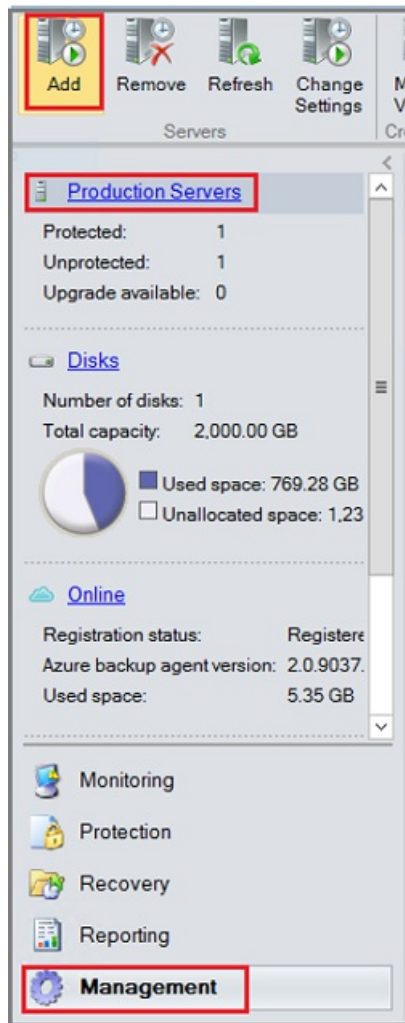
1. W vSphere klienta sieci Web, w menu **Nawigator**, kliknij przycisk **Administracja**.
2. W menu **Administracja** kliknij pozycję **Użytkownicy i grupy**.
3. Aby utworzyć nowego użytkownika, na karcie **Użytkownicy** kliknij przycisk "+", aby otworzyć okno dialogowe **nowego użytkownika**.
4. Podaj **nazwę użytkownika** i **hasło** dla roli. Użyj BackupAdmin jako nazwy użytkownika. Dodatkowe informacje są opcjonalne.

Przypisz rolę, BackupAdminRole do użytkownika, BackupAdmin

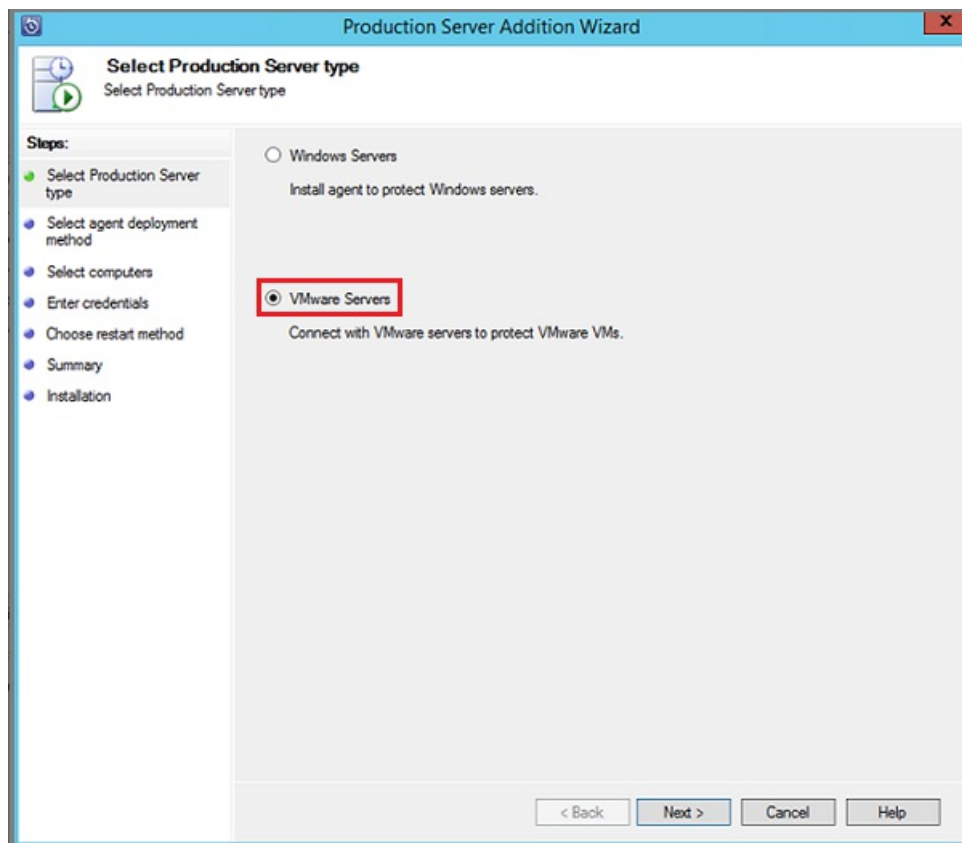
1. W vSphere klienta sieci Web, w menu Nawigator, kliknij przycisk **Administracja**.
2. W menu Administracja kliknij pozycję **uprawnienia globalne**.
3. W okienku **uprawnienia globalne** kliknij kartę **Zarządzanie**.
4. Na karcie **Zarządzanie** kliknij pozycję "+", aby otworzyć okno dialogowe **Dodawanie uprawnień**.
5. W oknie dialogowym **Dodawanie uprawnień** kliknij przycisk **Dodaj**.
6. W oknie dialogowym **Wybierz użytkowników/grupy** Wybierz poprawną domenę z menu **domena**, a następnie w kolumnie **użytkownik/Grupa** wybierz pozycję **BackupAdmin**, a następnie kliknij przycisk **Dodaj**. Nazwa użytkownika jest wyświetlana w polu Użytkownicy w formacie: domain\BackupAdmin.
7. Kliknij przycisk **OK**, aby powrócić do okna dialogowego Dodawanie uprawnień.
8. W obszarze **przypisana rola** z menu rozwijanego wybierz rolę, **BackupAdminRole**, a następnie kliknij przycisk **OK**. Nowy użytkownik i skojarzenie roli pojawiają się na karcie Zarządzanie.

Dodawanie serwera VMware do programu DPM

1. W Konsola administratora programu DPM kliknij pozycję **zarządzanie** > **serwery produkcyjne** > **Dodaj**, aby otworzyć Kreatora dodawania do serwera produkcyjnego.



2. Na **ekranie Wybieranie typu serwera produkcyjnego** wybierz pozycję **serwery VMware**, a następnie kliknij przycisk **dalej**.



3. Na ekranie **Wybieranie komputerów** podaj następujące informacje:

- **Nazwa/adres IP serwera:** wprowadź w pełni kwalifikowaną nazwę domeny (fQDN) serwera VMware lub adres IP.
- **Port SSL:** Wybierz numer portu SSL używany do komunikowania się z serwerem VMware. Program DPM komunikuje się z serwerami VMware za pośrednictwem zabezpieczonego połączenia przy użyciu protokołu HTTPS. Aby pomyślnie komunikować się z serwerami VMware, program DPM wymaga skonfigurowanego numeru portu SSL dla tego serwera VMware. Jeśli serwery VMware nie są jawnie skonfigurowane z różnymi portami SSL, przejdź do domyślnego portu 443.
- **Określ poświadczenie:** Wybierz poświadczenie, które jest konieczne do uwierzytelnienia na tym serwerze VMware. Jeśli wymagane poświadczenie nie zostało jeszcze dodane do programu DPM, wybierz pozycję **Dodaj nowe poświadczenie**. Następnie podaj nazwę, opis, nazwę użytkownika i hasło dla poświadczenia. Po wypełnieniu pól kliknij przycisk **Dodaj**, aby dodać serwer do listy serwerów VMware. Jeśli chcesz dodać więcej serwerów VMware do listy, Powtórz ten krok. Po zakończeniu dodawania serwerów do listy kliknij przycisk **dalej**.

4. Na ekranie **Podsumowanie** wybierz serwer, który chcesz dodać, a następnie kliknij przycisk **Dodaj**. Po dodaniu serwerów VMware do programu DPM, zobacz [Konfigurowanie kopii zapasowej](#), aby uzyskać informacje na temat dostępnych metod ochrony.

Wyłącz protokół bezpiecznej komunikacji

Jeśli Twoja organizacja nie chce korzystać z protokołu HTTPS, można utworzyć klucz rejestru, aby go wyłączyć. Aby utworzyć ten klucz rejestru:

1. Skopiuj i wklej następujący tekst do pliku txt.

```
Windows Registry Editor Version 5.00
```

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft Data Protection Manager\VMWare]
```

```
"IgnoreCertificateValidation"=dword:00000001
```

2. Zapisz plik o nazwie **DisableSecureAuthentication.reg** na serwerze DPM.

3. Kliknij dwukrotnie plik, aby aktywować wpis rejestru.

Konfiguruj kopię zapasową

Po dodaniu serwerów VMware do programu DPM prawie gotowe do rozpoczęcia ochrony w programie DPM. Jednak przed rozpoczęciem ochrony należy przydzielić magazyn dyskowy, który może być używany przez program DPM do przechowywania krótkoterminowego. Aby uzyskać wskazówki dotyczące dodawania magazynu, zobacz [Dodawanie magazynu do programu DPM](#). Po dodaniu magazynu można przystąpić do tworzenia grupy ochrony dla maszyn wirtualnych VMware za pomocą kreatora **tworzenia nowej grupy ochrony**.

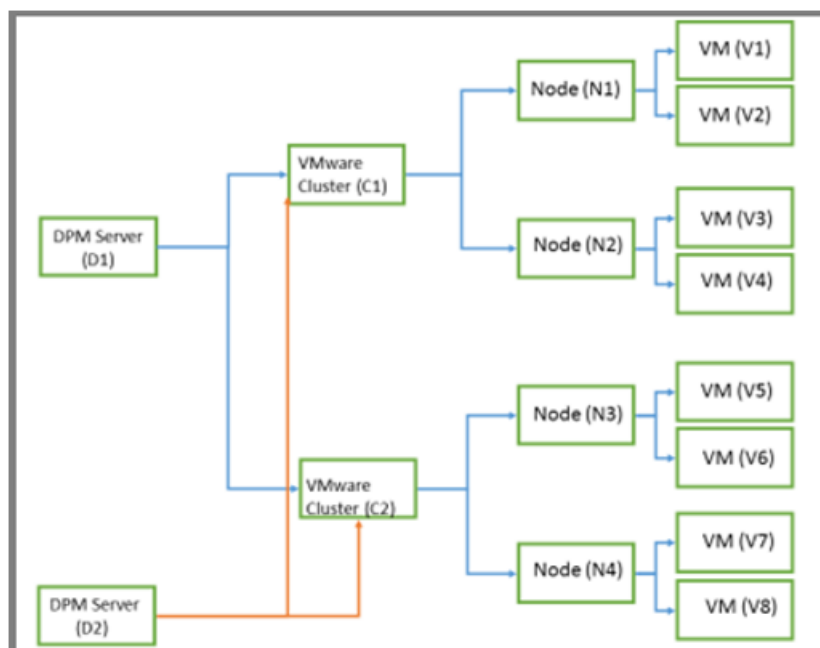
Ochrona na poziomie folderu

Program VMware udostępnia foldery maszyn wirtualnych, które umożliwiają organizowanie maszyn wirtualnych.

Program DPM może chronić poszczególne maszyny wirtualne, a także kaskadowe poziomy folderów, które zawierają maszyny wirtualne. Po wybraniu folderu do ochrony wszystkie foldery (i maszyny wirtualne) w tym folderze są automatycznie wykrywane i chronione. Jest to tzw. Ochrona na poziomie folderów. Program DPM wykrywa i konfiguruje ochronę maszyn wirtualnych na 12 godzin (w oparciu o lokalną strefę czasową serwera DPM). Gdy program DPM wykryje, że utworzono nowe maszyny wirtualne, program DPM skonfiguruje ochronę przed końcem tego dnia.

Skalowanie w poziomie ochrony klastrowanych serwerów VMware

W dużych wdrożeniach programu VMware pojedynczy serwer vCenter może zarządzać tysiącami maszyn wirtualnych. Program DPM obsługuje skalowalną w poziomie ochronę klastrów serwerów VMware. Nowa funkcja skalowania w poziomie usuwa ograniczenie relacji jeden-do-jednego między klastrem VMware a serwerem DPM. Maszynę wirtualną można dodać do grupy ochrony na dowolnym rozpoznanym serwerze programu DPM. Wiele serwerów DPM może służyć do ochrony maszyn wirtualnych zarządzanych przez pojedynczy serwer vCenter. Jednak tylko jeden serwer DPM może chronić maszynę wirtualną lub folder w danym momencie. Maszyny wirtualne i foldery, które są już chronione przez jeden serwer DPM, nie mogą zostać wybrane przez inny serwer DPM. Aby wdrożyć ochronę skalowalną w poziomie, muszą być dostępne co najmniej dwa serwery programu DPM. W poniższym przykładzie grafika D1 i D2 są widoczne dla wszystkich maszyn wirtualnych hostowanych w węzłach N1, N2, N3 i N4. Po utworzeniu grup ochrony na D1 lub D2 można dodać dowolną maszynę wirtualną.



Tworzenie kopii zapasowych maszyn wirtualnych na dysku, na taśmie lub w chmurze

Program DPM może tworzyć kopie zapasowe maszyn wirtualnych VMware na dysku, na taśmie i w chmurze platformy Azure. Podczas tworzenia nowej grupy ochrony należy określić metodę ochrony.

W przypadku wszystkich scenariuszy odzyskiwania operacyjnego, takich jak przypadkowe usunięcie lub scenariusze uszkodzeń, należy wykonać kopię zapasową na dysku. Aby uzyskać długoterminowe przechowywanie lub wymagania dotyczące kopii zapasowych poza siedzibą firmy, wykonaj kopię zapasową na [taśmie](#) lub w [chmurze](#).

Program DPM zapewnia spójne z aplikacjami kopie zapasowe maszyn wirtualnych z systemem Windows oraz kopie zapasowe spójnych plików maszyn wirtualnych z systemem Linux (pod warunkiem zainstalowania narzędzi VMware na gościu).

Tworzenie kopii zapasowej maszyny wirtualnej na taśmie

NOTE

Dotyczy programu DPM 2019

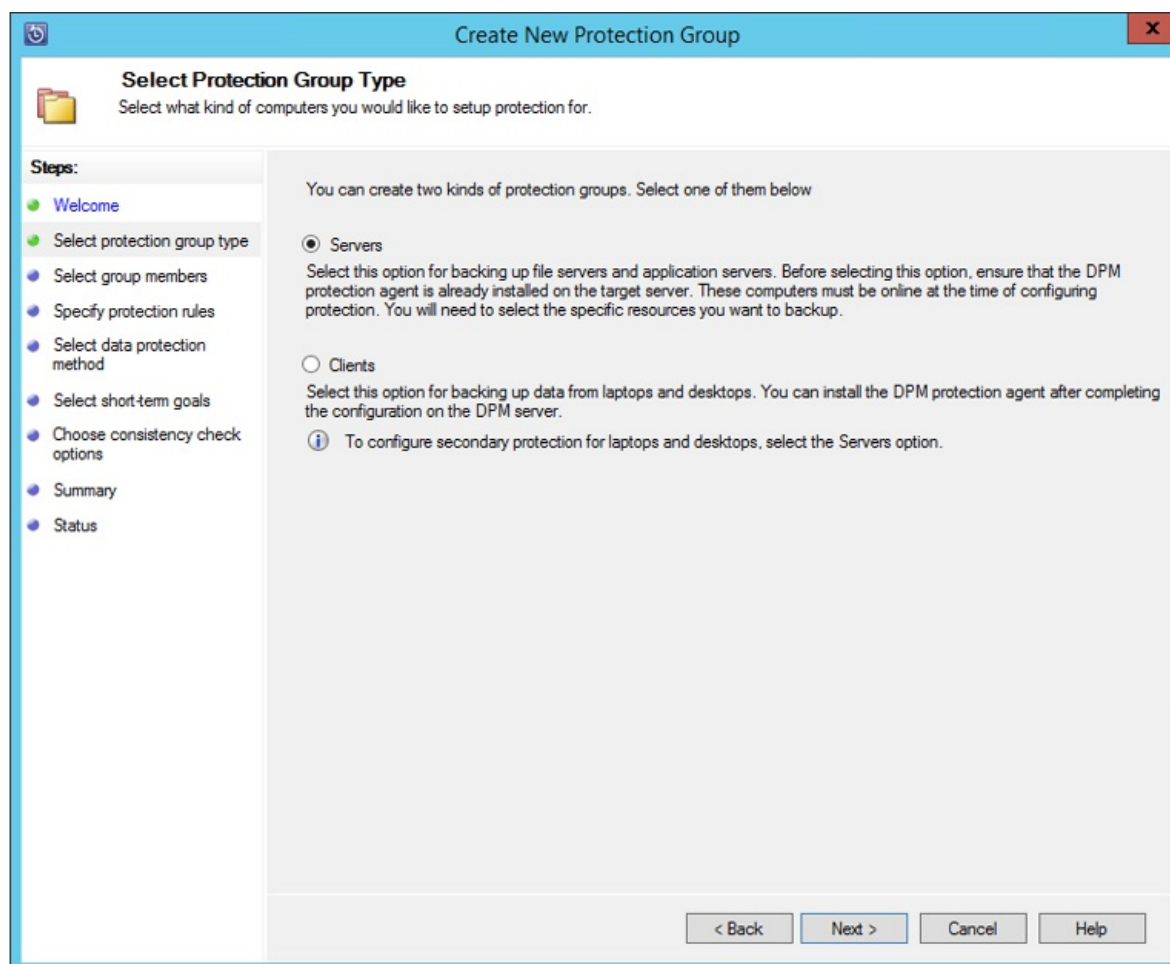
Do długoterminowego przechowywania danych kopii zapasowej programu VMware można teraz włączyć kopie zapasowe programu VMware na taśmie. Częstotliwość tworzenia kopii zapasowych można wybrać na podstawie zakresu przechowywania (co będzie różnić się od 1-99 lat) na stacjach taśm. Dane na stacjach taśm mogą być kompresowane i szyfrowane. Program DPM 2019 obsługuje zarówno OLR (oryginalna Lokalizacja odzyskiwania), & ALR (odzyskiwanie do lokalizacji alternatywnej) do przywracania chronionej maszyny wirtualnej.

Wykonaj następującą procedurę:

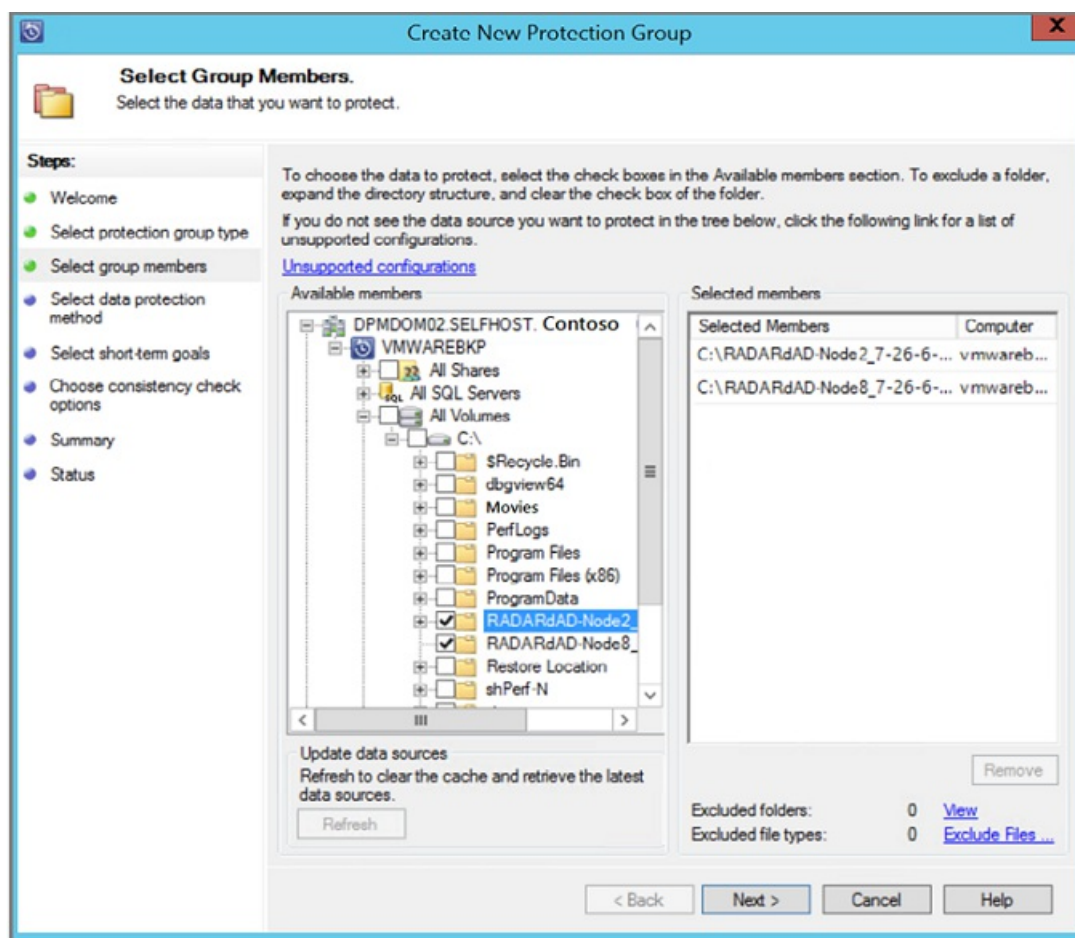
1. W konsoli administratora programu DPM kliknij pozycję **ochrona > Utwórz grupę ochrony**, aby otworzyć Kreatora tworzenia nowej grupy ochrony.
2. Na stronie **Wybierz członków grupy** Wybierz Maszyny wirtualne VMware, które chcesz chronić.
3. Na stronie **Wybierz metodę ochrony danych** wybierz opcję **Chcę uzyskać długoterminową ochronę za pomocą taśmy**.
4. W obszarze **Określ cele długoterminowe > Zakres przechowywania** Określ, jak długo chcesz przechowywać dane na taśmie (1-99 lat). W obszarze częstotliwość wykonywania kopii zapasowych wybierz żadaną częstotliwość tworzenia kopii zapasowych.
5. Na stronie **Wybieranie szczegółów taśmy i biblioteki** Określ taśmę i bibliotekę, która będzie używana do tworzenia kopii zapasowych tej grupy ochrony. Można również określić, czy dane kopii zapasowych mają być kompresowane lub szyfrowane.

Tworzenie grupy ochrony dla maszyn wirtualnych VMware

1. W konsola administratora kliknij pozycję **Ochrona**.
2. Na Wstążce narzędzi kliknij przycisk **New (nowy)**, aby otworzyć kreatora **tworzenia nowej grupy ochrony**.
3. Na ekranie **Wybierz typ grupy ochrony** wybierz pozycję **serwery**, a następnie kliknij przycisk **dalej**.



4. Na ekranie **Wybieranie członków grupy** rozwiń foldery **dostępne elementy członkowskie** i wybierz foldery, które mają być chronione, a następnie kliknij przycisk **dalej**. Po wybraniu folderu członek zostanie dodany do listy wybranych członków. Elementy, które są już chronione przez serwer programu DPM, nie mogą być ponownie wybrane. Wyświetl serwer programu DPM, który chroni element, umieszczając wskaźnik myszy na elemencie na liście dostępne elementy członkowskie.



5. Na ekranie **Wybierz metodę ochrony danych** wpisz **nazwę grupy ochrony**, a następnie wybierz metodę ochrony. W celu uzyskania metody ochrony można wybrać: krótkoterminową ochronę na dysku twardym, długoterminową kopię zapasową na taśmie lub ochronę online do chmury. Po wybraniu metody ochrony kliknij przycisk **dalej**.

Jeśli do serwera programu DPM jest podłączona taśma autonomiczna lub Biblioteka taśm, można wybrać opcję **Chcę uzyskać długoterminową ochronę za pomocą taśmy**.

6. Na ekranie **Określ cele krótkoterminowe dla zakresu przechowywania** Określ liczbę dni przechowywania danych na dysku. Jeśli chcesz zmienić harmonogram, gdy są pobierane punkty odzyskiwania aplikacji, kliknij przycisk **Modyfikuj**. Na karcie ekspresowa pełna kopia zapasowa wybierz nowy harmonogram dla czasu i dni tygodnia w przypadku wykonywania ekspresowych pełnych kopii zapasowych. Wartość domyślna to godzina 8 PM, czas lokalny dla serwera programu DPM. Jeśli masz cele krótkoterminowe, kliknij przycisk **dalej**.
7. Jeśli chcesz przechowywać dane na taśmie w celu przechowywania długoterminowego, w obszarze **Określ cele długoterminowe** wskaż, jak długo chcesz przechowywać dane na taśmie (1-99 lat). W obszarze **częstotliwość wykonywania kopii zapasowych** Określ, jak często mają być uruchamiane kopie zapasowe na taśmie. Częstotliwość zależy od wybranego zakresu przechowywania:

- Gdy zakres przechowywania wynosi 1–99 lat, można wybrać tworzenie kopii zapasowej codziennie, co tydzień, co dwa tygodnie, co miesiąc, co kwartał, co pół roku lub co rok.
- Gdy zakres przechowywania wynosi 1–11 miesięcy, można wybrać tworzenie kopii zapasowej codziennie, co tydzień, co dwa tygodnie lub co miesiąc.
- Gdy zakres przechowywania wynosi 1–4 tygodnie, można wybrać tworzenie kopii zapasowej codziennie lub co tydzień.

W przypadku korzystania z autonomicznej stacji taśm dla pojedynczej grupy ochrony program DPM używa tej samej taśmy do codziennego wykonywania kopii zapasowych do momentu, gdy zabraknie na niej miejsca. Można także rozróżnić dane z różnych grup ochrony na taśmie.

Na stronie **Wybieranie szczegółów taśmy i biblioteki** Określ taśmę/bibliotekę, która ma być używana, oraz czy dane mają być kompresowane i zyfrowane na taśmie.

8. Na ekranie **Przejrzyj przydział dysku** są wyświetlane zalecane przydziały dysku. Zalecenia są określone na podstawie zakresu przechowywania, typu obciążenia i rozmiaru chronionych danych. Kliknij przycisk **Dalej**.
9. Na ekranie **Wybieranie metody tworzenia repliki** Określ, jak ma zostać wykonana początkowa replikacja danych w grupie ochrony. W przypadku wybrania replikacji przez sieć zalecamy wybranie czasu poza godzinami szczytu. W przypadku dużych ilości danych lub nieoptymalnych warunków sieciowych należy wziąć pod uwagę replikację danych w trybie offline za pomocą nośników wymiennych.
10. Na ekranie **Opcje sprawdzania spójności** wybierz sposób automatyzacji sprawdzania spójności. Można włączyć uruchamianie sprawdzania tylko wtedy, gdy dane są niespójne, lub zgodnie z harmonogramem. Jeśli nie chcesz konfigurować automatycznego sprawdzania spójności, możesz uruchomić sprawdzanie ręczne. Aby uruchomić sprawdzanie ręczne, kliknij prawym przyciskiem myszy grupę ochrony w obszarze Ochrona w konsoli programu DPM, a następnie wybierz polecenie **Przeprowadź sprawdzanie spójności**.
11. Na ekranie **określanie danych ochrony online** wybierz źródła danych, które chcesz chronić.
12. Na ekranie **Określanie harmonogramu tworzenia kopii zapasowych online** Określ, jak często chcesz utworzyć kopię zapasową z kopii zapasowej dysku na platformie Azure. Punkt odzyskiwania jest tworzony za każdym razem, gdy wykonywana jest kopia zapasowa.
13. Na ekranie **Określanie zasad przechowywania w trybie online** Określ, jak długo chcesz przechowywać dane na platformie Azure. Więcej informacji na temat tworzenia kopii zapasowych programu DPM na platformie Azure można znaleźć w artykule [Tworzenie kopii zapasowych obciążeń programu DPM za pomocą Azure Backup](#).
14. Na ekranie wybierz replikację online wybierz metodę tworzenia początkowej kopii zapasowej. Domyślnie wybrana jest opcja wysyłania początkowej kopii zapasowej danych za pośrednictwem sieci. Jednak w przypadku dużej ilości danych korzystanie z funkcji kopii zapasowej offline może być bardziej czasochłonne. Zobacz artykuł [kopia zapasowa offline na platformie Azure](#), aby uzyskać więcej informacji, w tym przewodnik krok po kroku.
15. Na ekranie Podsumowanie przejrzyj ustawienia. Jeśli interesuje Cię Optymalizacja wydajności grupy ochrony, zapoznaj się z artykułem [Optymalizacja operacji programu DPM](#) wpływających na wydajność. Po spełnieniu wszystkich ustawień grupy ochrony kliknij pozycję **Utwórz grupę**, aby utworzyć grupę ochrony i wyzwolić początkową kopię zapasową.

Zostanie wyświetlony ekran stanu z aktualizacją tworzenia grupy ochrony oraz stanem początkowej kopii zapasowej.

Przywróć maszyny wirtualne VMware

W tej sekcji opisano, jak przywrócić [punkty odzyskiwania](#) maszyn wirtualnych VMware za pomocą programu DPM. Aby uzyskać przegląd dotyczący odzyskiwania danych przy użyciu programu DPM, zobacz [odzyskiwanie chronionych danych](#). W Konsola administratora programu DPM istnieją dwa sposoby znajdowania odzyskiwalnych danych — wyszukiwanie i przeglądanie. Podczas odzyskiwania danych można lub nie chcieć przywracać danych ani maszyn wirtualnych do tej samej lokalizacji. Z tego powodu program DPM obsługuje trzy opcje odzyskiwania kopii zapasowych maszyn wirtualnych VMware.

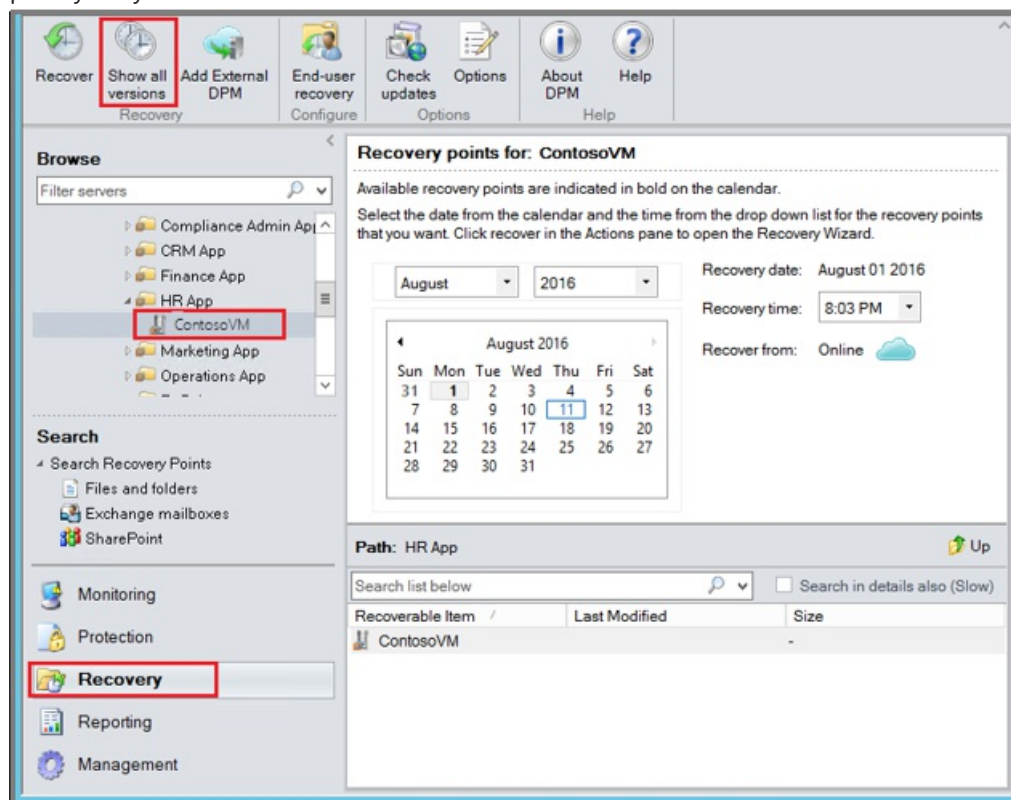
- **Odzyskiwanie do oryginalnej lokalizacji (OLR)** — umożliwia przywrócenie chronionej maszyny wirtualnej do jej oryginalnej lokalizacji przy użyciu funkcji OLR. Maszynę wirtualną można przywrócić do jej oryginalnej lokalizacji tylko wtedy, gdy nie dodano ani nie usunięto dysków, ponieważ wystąpiła kopia zapasowa. Jeśli dyski zostały dodane lub usunięte, musisz użyć odzyskiwania do lokalizacji alternatywnej.
- **Odzyskiwanie do lokalizacji alternatywnej (ALR)** — gdy brakuje oryginalnej maszyny wirtualnej lub nie chcesz zakłócać oryginalnej maszyny wirtualnej, ODZYSKAJ maszynę wirtualną do lokalizacji alternatywnej. Aby odzyskać maszynę wirtualną do lokalizacji alternatywnej, należy podać lokalizację hosta ESXi, puli zasobów, folderu oraz magazynu danych magazynu i ścieżki. Aby ułatwić odróżnienie przywróconej maszyny

wirtualnej od oryginalnej maszyny wirtualnej, program DPM dołącza "-Odzyskaj" do nazwy maszyny wirtualnej.

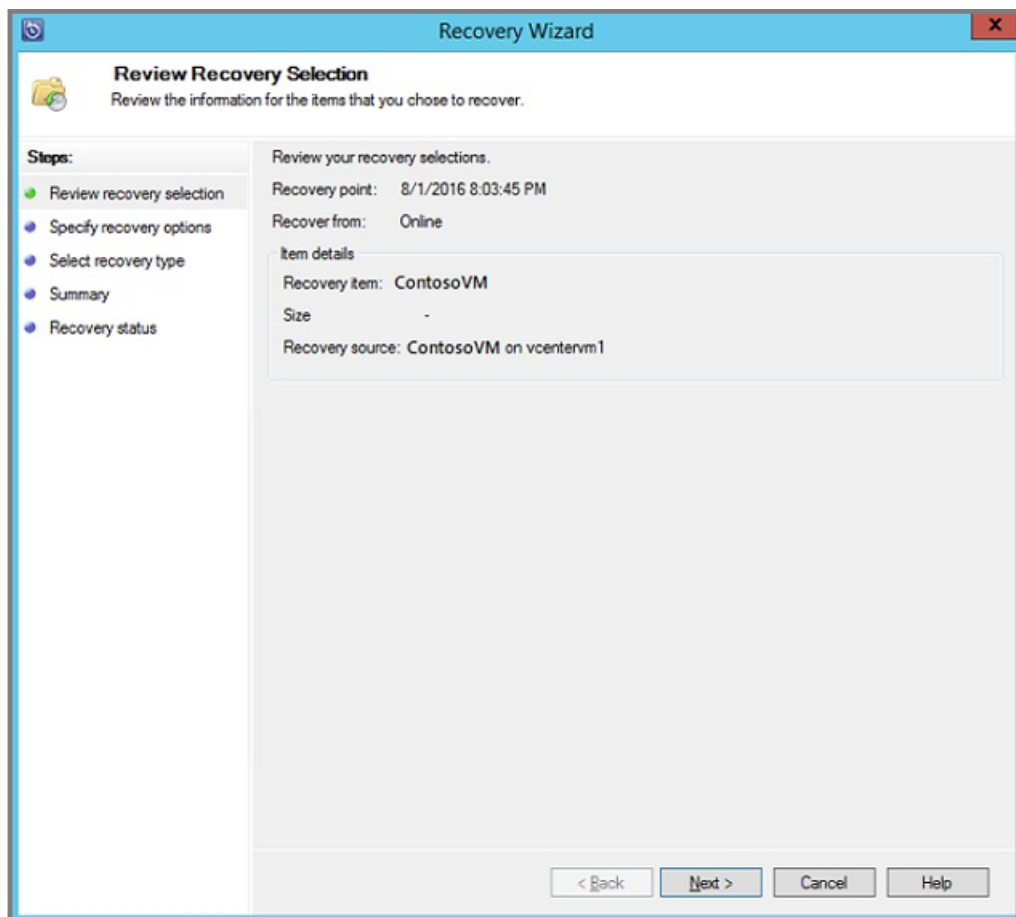
- **Odzyskiwanie poszczególnych lokalizacji plików (ILR)** — Jeśli chroniona maszyna wirtualna jest maszyną wirtualną z systemem Windows Server, można odzyskać pojedyncze pliki/foldery w ramach maszyny wirtualnej przy użyciu funkcji ILR programu DPM. Aby odzyskać poszczególne pliki, zapoznaj się z procedurą w dalszej części tego artykułu.

Przywracanie punktu odzyskiwania

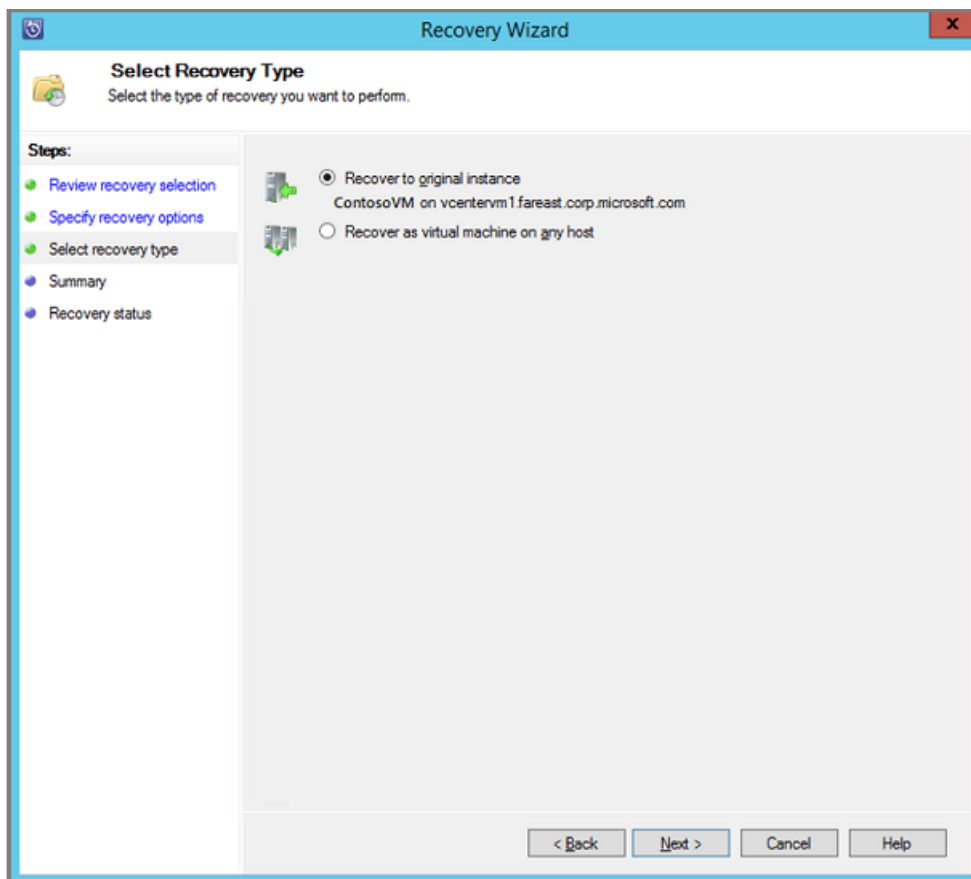
1. W Konsola administratora programu DPM kliknij pozycję Widok **odzyskiwania**.
2. Za pomocą okienka przeglądania Przeglądaj lub Filtruj, aby znaleźć maszynę wirtualną, którą chcesz odzyskać. Po wybraniu maszyny wirtualnej lub folderu punkty odzyskiwania w okienku zostaną wyświetlone dostępne punkty odzyskiwania.



3. W polu **punkty odzyskiwania dla** Użyj menu kalendarz i listy rozwijanej, aby wybrać datę utworzenia punktu odzyskiwania. Pogrubienie dat kalendarza ma dostępne punkty odzyskiwania.
4. Na Wstążce narzędzi kliknij polecenie **Odzyskaj**, aby otworzyć **Kreatora odzyskiwania**.



5. Kliknij przycisk **dalej** , aby przejść do ekranu **Określanie opcji odzyskiwania** .
6. Aby włączyć ograniczanie przepustowości sieci, na ekranie **Określ opcje odzyskiwania** kliknij przycisk **Modyfikuj**. Aby wyłączyć funkcję ograniczania przepustowości sieci, kliknij przycisk **dalej**. Dla maszyn wirtualnych VMware nie są dostępne żadne inne opcje na tym ekranie kreatora. Jeśli zdecydujesz się zmodyfikować przepustowość sieci, w oknie dialogowym ograniczenia wybierz opcję **Włącz ograniczenie przepustowości sieci** , aby je włączyć. Po włączeniu Skonfiguruj **Ustawienia i harmonogram pracy**.
7. Na ekranie **Wybieranie typu odzyskiwania** wybierz, czy chcesz odzyskać do oryginalnego wystąpienia, czy też do nowej lokalizacji, a następnie kliknij przycisk **dalej**.
 - W przypadku wybrania opcji **Odzyskaj do oryginalnego wystąpienia** trzeba wprowadzać więcej opcji w kreatorze. Dane dla oryginalnego wystąpienia są używane.
 - Jeśli wybierzesz opcję **Odzyskaj jako maszynę wirtualną na dowolnym hoście**, na ekranie **określ miejsce docelowe** podaj informacje dotyczące **hosta ESXi, puli zasobów, folderu i ścieżki**.

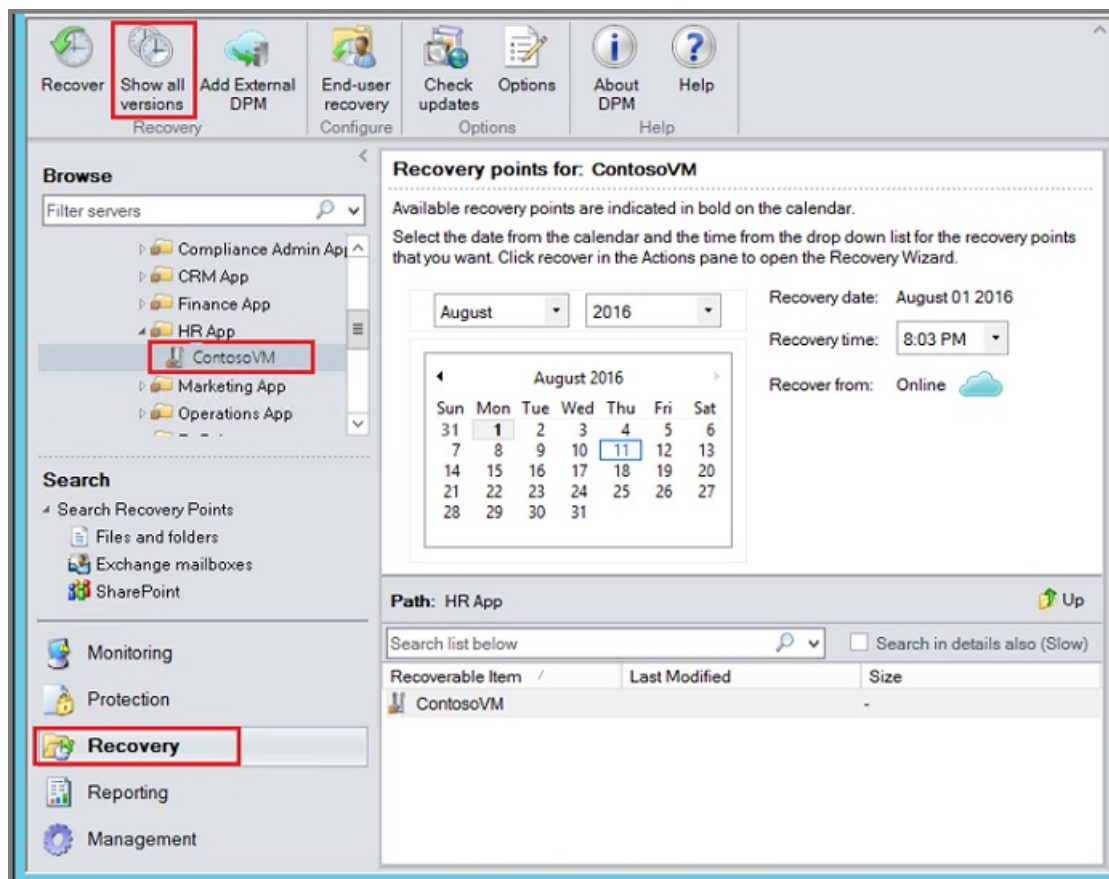


8. Na ekranie **Podsumowanie** przejrzyj ustawienia, a następnie kliknij przycisk **Odzyskaj** , aby rozpocząć proces odzyskiwania. Ekran **stan odzyskiwania** pokazuje postęp operacji odzyskiwania.

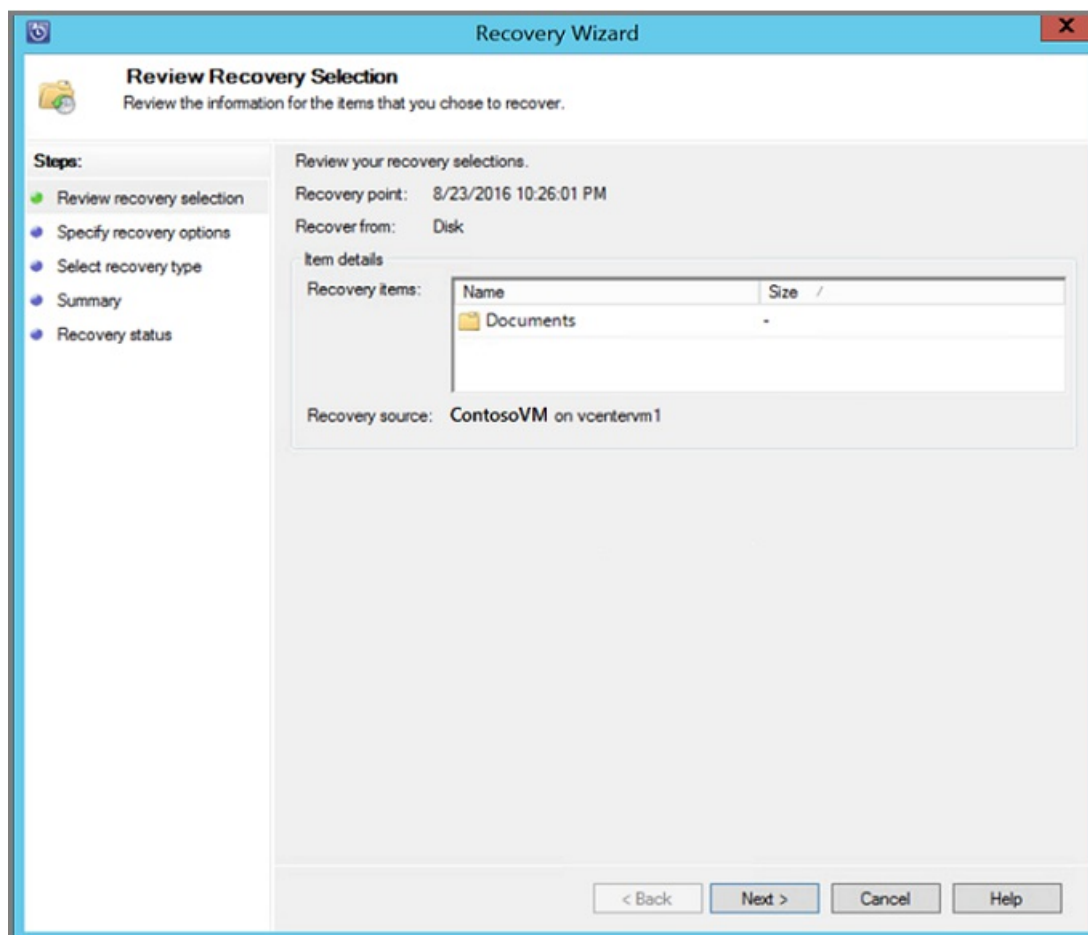
Przywracanie pojedynczego pliku z maszyny wirtualnej

Można przywrócić pojedyncze pliki z chronionego punktu odzyskiwania maszyny wirtualnej. Ta funkcja jest dostępna tylko dla maszyn wirtualnych z systemem Windows Server. Przywracanie pojedynczych plików jest podobne do przywracania całej maszyny wirtualnej, z tą różnicą, że przed rozpoczęciem procesu odzyskiwania przejdiesz do dysku VMDK i wyszukasz żądane pliki. Aby odzyskać pojedynczy plik lub wybrać pliki z maszyny wirtualnej z systemem Windows Server:

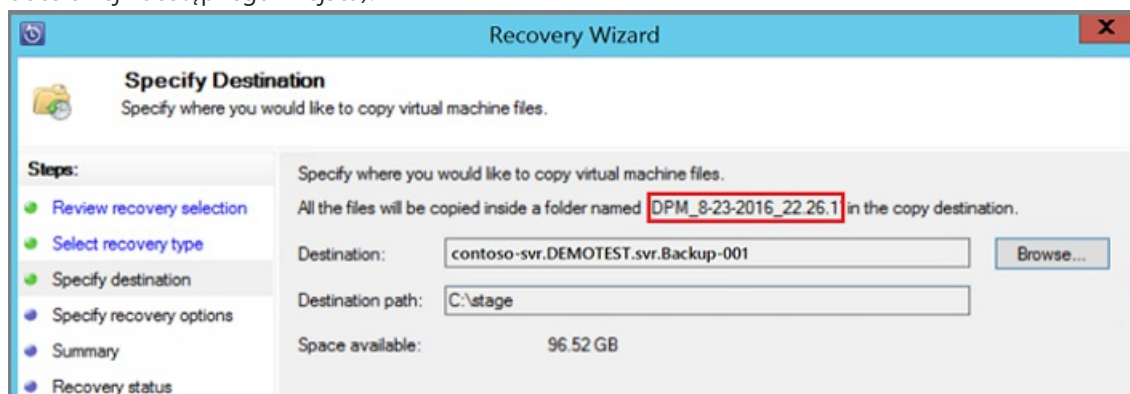
1. W Konsola administratora programu DPM kliknij pozycję Widok **odzyskiwania** .
2. Za pomocą okienka **przeglądania** Przeglądaj lub Filtruj, aby znaleźć maszynę wirtualną, którą chcesz odzyskać. Po wybraniu maszyny wirtualnej lub folderu punkty odzyskiwania w okienku zostaną wyświetlone dostępne punkty odzyskiwania.



3. W okienku **punkty odzyskiwania dla:** Użyj kalendarza, aby wybrać datę zawierającą żądane punkty odzyskiwania. W zależności od sposobu skonfigurowania zasad tworzenia kopii zapasowych daty mogą mieć więcej niż jeden punkt odzyskiwania. Po wybraniu dnia, w którym wykonano punkt odzyskiwania, upewnij się, że wybrano prawidłowy czas odzyskiwania. Jeśli wybrana data ma wiele punktów odzyskiwania, wybierz punkt odzyskiwania, wybierając go z menu rozwijanego **godzina odzyskiwania** . Po wybraniu punktu odzyskiwania zostanie wyświetlona lista elementów możliwych do odzyskania w okienku **ścieżka:** .
4. Aby znaleźć pliki do odzyskania, w okienku **ścieżki** kliknij dwukrotnie element w kolumnie element możliwy do **odzyskania** , aby go otworzyć. Wybierz plik, pliki lub foldery, które chcesz odzyskać. Aby zaznaczyć wiele elementów, naciśnij klawisz **Ctrl** podczas zaznaczania każdego elementu. Użyj okienka **ścieżka** , aby przeszukać listę plików lub folderów wyświetlanych w kolumnie element możliwy do **odzyskania** . **Poniższa lista wyszukiwania** nie przeszukuje podfolderów. Aby przeszukać podfoldery, kliknij dwukrotnie folder. Użyj przycisku do **góry** , aby przejść z folderu podrzędnego do folderu nadrzędnego. Można wybrać wiele elementów (plików i folderów), ale muszą one znajdować się w tym samym folderze nadrzędnym. Nie można odzyskać elementów z wielu folderów w ramach tego samego zadania odzyskiwania.
5. Po wybraniu elementów do odzyskania na Wstążce narzędzia konsola administratora kliknij przycisk **Odzyskaj** , aby otworzyć **Kreatora odzyskiwania**. W Kreatorze odzyskiwania ekran **Przegląd opcji odzyskiwania** pokazuje wybrane elementy do odzyskania.



6. Aby włączyć ograniczanie przepustowości sieci, na ekranie **Określ opcje odzyskiwania** kliknij przycisk **Modyfikuj**. Aby wyłączyć funkcję ograniczania przepustowości sieci, kliknij przycisk **dalej**. Dla maszyn wirtualnych VMware nie są dostępne żadne inne opcje na tym ekranie kreatora. Jeśli zdecydujesz się zmodyfikować przepustowość sieci, w oknie dialogowym ograniczenia wybierz opcję **Włącz ograniczenie przepustowości sieci**, aby je włączyć. Po włączeniu Skonfiguruj **Ustawienia i harmonogram pracy**.
7. Na ekranie **Wybieranie typu odzyskiwania** kliknij przycisk **dalej**. Pliki lub foldery można odzyskiwać tylko do folderu sieciowego.
8. Na ekranie **określ miejsce docelowe** kliknij przycisk **Przeglądaj**, aby znaleźć lokalizację sieciową dla plików lub folderów. Program DPM tworzy folder, w którym są kopiowane wszystkie odzyskane elementy. Nazwa folderu ma prefiks, DPM_day-miesiąc — rok. W przypadku wybrania lokalizacji odzyskiwanych plików lub folderów zostaną podane szczegóły dotyczące tej lokalizacji (lokalizacji docelowej, ścieżki docelowej i dostępnego miejsca).



9. Na stronie **Określ opcje odzyskiwania** wybierz ustawienia zabezpieczeń, które mają zostać zastosowane. Można wybrać opcję modyfikacji ograniczenia przepustowości sieci, ale ograniczenie przepustowości jest domyślnie wyłączone. Ponadto odzyskiwanie i **powiadamanie sieci San** nie są włączone.

10. Na ekranie **Podsumowanie** przejrzyj ustawienia, a następnie kliknij przycisk **Odzyskaj**, aby rozpocząć proces odzyskiwania. **Ekran stan odzyskiwania pokazuje postęp operacji odzyskiwania.**

Równoległe kopie zapasowe VMware

W starszych wersjach programu DPM równoległe kopie zapasowe były wykonywane tylko w grupach ochrony. W przypadku programu DPM 2019 wszystkie kopie zapasowe maszyn wirtualnych VMWare w ramach jednej grupy ochrony są równoległe, co prowadzi do szybszego tworzenia kopii zapasowych maszyn wirtualnych. Wszystkie zadania replikacji różnicowej programu VMWare będą wykonywane równoległe. Domyślnie liczba zadań do uruchomienia równoległego jest ustawiona na 8.

Liczbę zadań można zmodyfikować przy użyciu klucza rejestru, jak pokazano poniżej (nieobecny domyślnie, należy dodać):

Ścieżka klucza : Software\Microsoft\Microsoft Data Protection Manager\Configuration\MaxParallelIncrementalJobs\VMWare **klucza** : wartość DWORD (32-bitowa).

NOTE

Liczbę zadań można zmodyfikować na wyższą wartość. W przypadku ustawienia numeru zadania na 1 zadania replikacji są uruchamiane sekwencyjnie. Aby zwiększyć liczbę do wyższej wartości, należy wziąć pod uwagę wydajność programu VMWare. Biorąc pod uwagę liczbę używanych zasobów i dodatkowe użycie wymagane na serwerze VMWare vSphere, należy określić liczbę zadań replikacji różnicowej, które mają być uruchamiane równoległe. Ponadto ta zmiana będzie miała wpływ tylko na nowo utworzone grupy ochrony. W przypadku istniejących grup ochrony należy tymczasowo dodać kolejną maszynę wirtualną do grupy ochrony. Należy odpowiednio zaktualizować konfigurację grupy ochrony. Po zakończeniu procedury można usunąć tę maszynę wirtualną z grupy ochrony.

VMWare vSphere 6,7

Aby utworzyć kopię zapasową vSphere 6,7, wykonaj następujące czynności:

- Włącz protokół TLS 1,2 na serwerze DPM

NOTE

Oprogramowanie VMWare 6,7 z włączoną obsługą protokołu TLS jako protokół komunikacyjny.

- Ustaw klucze rejestru w następujący sposób:

Edytor rejestru systemu Windows w wersji 5,00

[HKEY_LOCAL_MACHINE \SOFTWARE\WOW6432Node\Microsoft\ .NETFramework\v2.0.50727]
"SystemDefaultTlsVersions" = DWORD: 00000001 "Schusestrongcrypto we" = DWORD: 00000001

[HKEY_LOCAL_MACHINE \SOFTWARE\WOW6432Node\Microsoft\ .NETFramework\v4.0.30319]
"SystemDefaultTlsVersions" = DWORD: 00000001 "Schusestrongcrypto we" = DWORD: 00000001

[HKEY_LOCAL_MACHINE \SOFTWARE\Microsoft\ .NETFramework\v2.0.50727]
"SystemDefaultTlsVersions" = DWORD: 00000001 "Schusestrongcrypto we" = DWORD: 00000001

[HKEY_LOCAL_MACHINE \SOFTWARE\Microsoft\ .NETFramework\v4.0.30319]
"SystemDefaultTlsVersions" = DWORD: 00000001 s "Schusestrongcrypto we" = DWORD: 00000001

Wyklucz dysk z kopii zapasowej maszyny wirtualnej VMware

NOTE

Ta funkcja ma zastosowanie do programu DPM 2019 UR1.

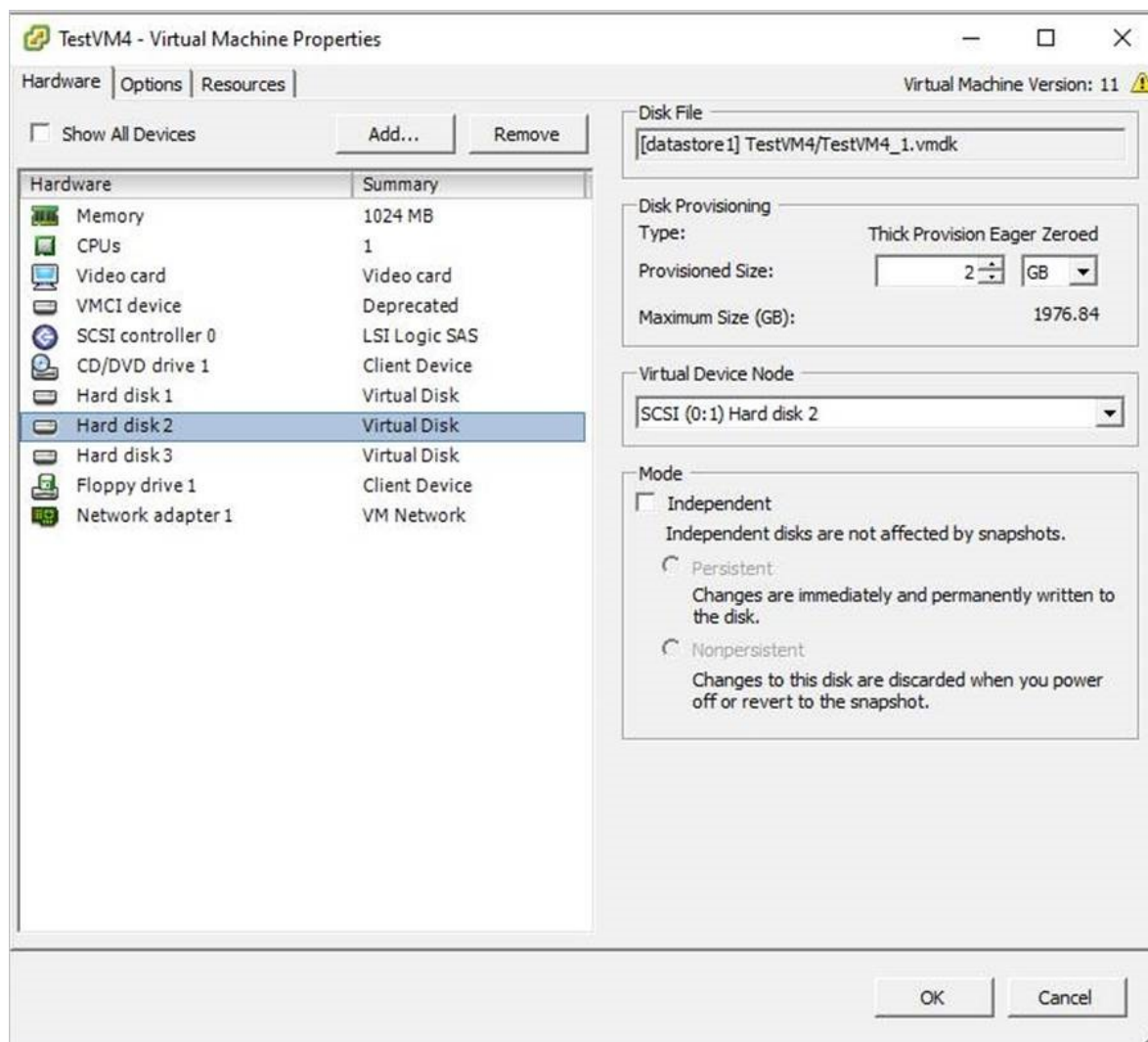
Program DPM 2019 UR1 umożliwia wykluczenie określonego dysku z kopii zapasowej maszyny wirtualnej VMware. Skrypt konfiguracyjny **ExcludeDisk.ps1** znajduje się w folderze C:\Program Files\Microsoft System Center\DPM\DPM\bin.

Aby skonfigurować wykluczenie dysku, wykonaj następujące czynności:

Zidentyfikuj szczegóły maszyny wirtualnej VMWare i dysku do wykluczenia

1. W konsoli programu VMware przejdź do ustawień maszyny wirtualnej, dla których chcesz wykluczyć dysk.
2. Wybierz dysk, który ma zostać wykluczony, i Zannotuj ścieżkę dla tego dysku.

Na przykład aby wykluczyć dysk twardey 2 z TestVM4, ścieżka do dysku twardego 2 to **[datastore1] TestVM4/TestVM4_1.vmdk**.



Konfigurowanie serwera DPM

Przejdź do serwera programu DPM, na którym skonfigurowano maszynę wirtualną VMware do ochrony w celu skonfigurowania wykluczenia dysku.

1. Zapoznaj się ze szczegółami hosta VMware, który jest chroniony na serwerze DPM.

```
PS C:\>$psInfo = get-DPMProductionServer
PS C:\> $psInfo
```

ServerName	ClusterName	Domain	ServerProtectionState
-----	-----	-----	-----
Vcentervm1		Contoso.COM	NoDataSourcesProtected

2. Wybierz hosta VMware i Wyświetl listę ochrony maszyn wirtualnych dla hosta VMware.

```
PS C:\> $vmDsInfo = get-DPMDataSource -ProductionServer $psInfo[0] -Inquire
PS C:\> $vmDsInfo
```

Computer	Name	ObjectType
-----	----	-----
Vcentervm1	TestVM2	VMware
Vcentervm1	TestVM1	VMware
Vcentervm1	TestVM4	VMware

3. Wybierz maszynę wirtualną, dla której chcesz wykluczyć dysk.

```
PS C:\>$vmDsInfo[2]
```

Computer	Name	ObjectType
-----	----	-----
Vcentervm1	TestVM4	VMware

4. Aby wykluczyć dysk, przejdź do folderu bin i uruchom skrypt *ExcludeDisk.ps1* z następującymi parametrami:

NOTE

Przed uruchomieniem tego polecenia Zatrzymaj usługę DPMRA na serwerze programu DPM. W przeciwnym razie skrypt zwraca sukces, ale nie aktualizuje listy wykluczeń. Przed zatrzymaniem usługi upewnij się, że żadne zadania nie są w toku.

Aby dodać/usunąć dysk z wykluczenia, uruchom następujące polecenie:

```
./ExcludeDisk.ps1 -DataSource $vmDsInfo[0] [-Add|Remove] "[Datastore] vmdk/vmdk.vmdk"
```

Przykład: aby dodać wykluczenie dysku dla TestVM4, uruchom następujące polecenie

```
PS C:\Program Files\Microsoft System Center\DPM\DPM\bin> ./ExcludeDisk.ps1 -DataSource $vmDsInfo[2] -
Add "[datastore1] TestVM4/TestVM4\_1.vmdk"
Creating C:\Program Files\Microsoft System Center\DPM\DPM\bin\excludedisk.xml
Disk : [datastore1] TestVM4/TestVM4\_1.vmdk, has been added to disk exclusion list.
```

5. Sprawdź, czy dysk został dodany do wykluczenia

Aby wyświetlić istniejące wykluczenie dla określonych maszyn wirtualnych, uruchom następujące polecenie:

```
./ExcludeDisk.ps1 -DataSource $vmDsInfo[0] [-view]
```

Przykład

```
PS C:\Program Files\Microsoft System Center\DPM\DPM\bin> ./ExcludeDisk.ps1 -Datasource $vmDsInfo[2] -view
<VirtualMachine>
<UUID>52b2b1b6-5a74-1359-a0a5-1c3627c7b96a</UUID>
<ExcludeDisk>[datastore1] TestVM4/TestVM4\_1.vmdk</ExcludeDisk>
</VirtualMachine>
```

Po skonfigurowaniu ochrony dla tej maszyny wirtualnej dysk wykluczony nie będzie wyświetlany na liście podczas ochrony.

NOTE

Jeśli wykonujesz te kroki dla już chronionej maszyny wirtualnej, musisz ręcznie uruchomić sprawdzanie spójności po dodaniu dysku do wykluczenia.

Usunąć dysk z wykluczenia

Aby usunąć dysk z wykluczenia, uruchom następujące polecenie:

```
PS C:\Program Files\Microsoft System Center\DPM\DPM\bin> ./ExcludeDisk.ps1 -Datasource $vmDsInfo[2] -Remove "[datastore1] TestVM4/TestVM4\_1.vmdk"
```


Tworzenie i przywracanie kopii zapasowej serwerów VMM

10.01.2020 • 12 minutes to read

Program System Center Data Protection Manager (DPM) umożliwia tworzenie kopii zapasowych wystąpień SQL Server, które są używane jako baza danych programu System Center Virtual Machines Manager (VMM) na kilka sposobów:

- Regularne tworzenie kopii zapasowej programu SQL Server.
- Można utworzyć kopię zapasową bazy danych SQL Server przy użyciu składnika zapisywania programu VMM Express, który jest wyświetlany w obszarze serwer programu VMM w konsoli programu DPM. Główną zaletą tej metody jest to, że nie trzeba konfigurować żadnych specjalnych uprawnień w programie SQL Server.

Program DPM może tworzyć kopie zapasowe bazy danych programu VMM przy użyciu składnika zapisywania ekspresowego VMM, gdy program VMM działa w pakiecie System Center 2012 lub nowszym jako maszyna fizyczna/wirtualna w następujących scenariuszach wdrożenia:

- Autonomiczny host programu VMM i autonomiczne wystąpienie programu SQL Server (domyślne i nazwane, lokalne i zdalne)
- Autonomiczny host programu VMM i klastrowane wystąpienie programu SQL Server (domyślne i nazwane, zdalne)
- Klastrowany host programu VMM i autonomiczne wystąpienie programu SQL Server (domyślne i nazwane, lokalne i zdalne)
- Klastrowany host programu VMM i klastrowane wystąpienie programu SQL Server (domyślne i nazwane, zdalne)

Wymagania wstępne i ograniczenia

Przed skonfigurowaniem kopii zapasowej dla programu VMM w programie DPM przy użyciu składnika zapisywania ekspresowego VMM należy pamiętać o następujących kwestiach:

- Program DPM tworzy wyłącznie kopię zapasową bazy danych programu SQL Server używanej przez program DPM. Nie tworzy kopii zapasowej wszystkich plików konfiguracji w bibliotece programu VMM.
- Program DPM obsługuje replikację początkową i ekspresowe pełne kopie zapasowe w przypadku maszyn programu VMM. Przyrostowe kopie zapasowe nie są obsługiwane.
- Program DPM nie utworzy kopii zapasowej bazy danych programu VMM, jeśli podczas konfigurowania programu VMM określono statyczny adres IP dla programu SQL Server. Program DPM również nie utworzy kopii zapasowej, jeśli określono wartość „localhost” dla bazy danych.
- W przypadku używania szyfrowania za pomocą rozproszonego zarządzania kluczami (klucz przechowywany w usłudze AD) program DPM nie utworzy kopii zapasowej klucza. Jego ochronę należy zapewnić w ramach tworzenia kopii zapasowej usługi AD. Jeśli klucz jest przechowywany lokalnie, jego kopia zapasowa jest tworzona w ramach kopii zapasowej bazy danych.
- Jeśli dojdzie do przełączenia w tryb failover, program DPM będzie kontynuował tworzenie kopii zapasowej, gdy węzeł programu VMM przejdzie w tryb online. Umożliwia to przeprowadzanie planowanych przełączeń

w tryb failover bez utraty ochrony. Jeśli jednak węzeł zostanie utracony, konieczne będzie skonfigurowanie kopii zapasowych dla nowego węzła.

- W przypadku hostów programu VMM program DPM obsługuje odzyskiwanie do oryginalnej lokalizacji. Odzyskiwanie do alternatywnej lokalizacji nie jest obsługiwane.

Przed rozpoczęciem

- Przeczytaj [informacje o wersji](#) oraz artykuł [What's supported and what isn't for DPM?](#) (Co jest obsługiwane przez program DPM, a co nie?), który opisuje problemy z tworzeniem kopii zapasowych w programie VMM.
- Upewnij się, że maszyny programu VMM, dla których mają być tworzone kopie zapasowe, znajdują się w domenie serwera programu DPM lub w domenie mającej dwukierunkową relację zaufania z domeną programu DPM.
- **Konfigurowanie magazynu** — dane kopii zapasowej można przechowywać na dysku, na taśmie i w chmurze przy użyciu platformy Azure. Więcej informacji znajduje się w temacie [Prepare data storage](#) (Przygotowanie magazynu danych).
- Należy wdrożyć agenta ochrony programu DPM na serwerze programu VMM. Aby dowiedzieć się więcej, zobacz [Deploy the DPM protection agent](#) (Wdrażanie agenta ochrony programu DPM).

Tworzenie kopii zapasowej programu VMM

1. Kliknij kolejno pozycje **Ochrona > Akcje > Utwórz grupę ochrony**, aby otworzyć kreatora **tworzenia nowej grupy ochrony** w konsoli programu DPM.
2. W obszarze **Wybór grupy ochrony** kliknij opcję **Klienci**. Opcję Klienci należy wybrać tylko wtedy, gdy chcesz utworzyć kopię zapasową danych komputera z wersją kliencką systemu operacyjnego Windows. W przypadku wszystkich innych obciążeń wybierz opcję Serwery. Aby dowiedzieć się więcej, zobacz [Deploy protection groups](#) (Wdrażanie grup ochrony).
3. W polu **Wybierz członków grupy** rozwiń maszynę programu VMM i wybierz pozycję **Składnik zapisywania ekspresowego VMM**.
4. W obszarze **Wybierz metodę ochrony danych** określ, jak mają być obsługiwane krótkoterminowe i długoterminowe kopie zapasowe. Krótkoterminowa kopia zapasowa jest zawsze najpierw tworzona na dysku z opcją przeniesienia kopii zapasowej z dysku do chmury platformy Azure za pomocą usługi Azure Backup (na potrzeby przechowywania krótkoterminowego lub długoterminowego). Zamiast długoterminowej kopii zapasowej w chmurze możesz również skonfigurować długoterminową kopię zapasową na autonomicznym urządzeniu taśmowym lub w bibliotece taśm połączonej z serwerem programu DPM.
5. W polu **Wybierz cele krótkoterminowe** określ sposób tworzenia kopii zapasowej w krótkoterminowym magazynie na dysku. W obszarze Zakres przechowywania określ, jak długo chcesz przechowywać dane na dysku. W obszarze **Częstotliwość synchronizacji** określ, jak często chcesz zapisywać przyrostowe kopie zapasowe na dysku. Jeśli nie chcesz ustawiać interwału kopii zapasowych, możesz zaznaczyć opcję Zaraz przed punktem odzyskiwania, aby program DPM wykonywał ekspresową pełną kopię zapasową bezpośrednio przed każdym zaplanowanym punktem odzyskiwania.
6. Jeśli chcesz utworzyć długoterminową kopię zapasową danych na taśmie, na stronie **Określ cele długoterminowe** wskaż, jak długo chcesz przechowywać dane na taśmie (od 1 roku do 99 lat). W obszarze Częstotliwość wykonywania kopii zapasowych określ, jak często mają być wykonywane kopie zapasowe na taśmie. Częstotliwość zależy od wybranego zakresu przechowywania:
 - Gdy zakres przechowywania wynosi 1–99 lat, można wybrać tworzenie kopii zapasowej codziennie, co tydzień, co dwa tygodnie, co miesiąc, co kwartał, co pół roku lub co rok.

- Gdy zakres przechowywania wynosi 1–11 miesięcy, można wybrać tworzenie kopii zapasowej codziennie, co tydzień, co dwa tygodnie lub co miesiąc.
- Gdy zakres przechowywania wynosi 1–4 tygodnie, można wybrać tworzenie kopii zapasowej codziennie lub co tydzień.

W przypadku korzystania z autonomicznej stacji taśm dla pojedynczej grupy ochrony program DPM używa tej samej taśmy do codziennego wykonywania kopii zapasowych do momentu, gdy zabraknie na niej miejsca. Na taśmie możesz również zapisywać dane z różnych grup ochrony.

Na stronie **Określanie szczegółów taśmy i biblioteki** określ taśmę lub bibliotekę, która ma być używana, oraz czy dane na taśmie mają być kompresowane i szyfrowane.

7. Na stronie **Przejrzyj przydział dysku** przejrzyj miejsce na dysku w puli magazynów przydzielone danej grupie ochrony. W obszarze **Rozmiar danych** jest wyświetlany rozmiar danych, dla których ma zostać utworzona kopia zapasowa, a w obszarze **Miejsce na dysku** jest widoczna ilość miejsca zalecanego przez program DPM dla grupy ochrony. Wybierz opcję **Automatycznie rozszerzaj woluminy**, aby automatycznie zwiększać rozmiar, gdy do wykonywania kopii zapasowych danych potrzeba więcej miejsca.
8. W polu **Wybierz metodę tworzenia repliki** określ, jak chcesz obsługiwać początkową pełną replikację danych. W przypadku wybrania replikowania za pośrednictwem sieci zaleca się wybranie czasu w godzinach małego obciążenia sieci. W przypadku dużych ilości danych lub nieoptymalnych warunków sieciowych należy wziąć pod uwagę replikację danych w trybie offline za pomocą nośników wymiennych.
9. W polu **Wybierz opcje sprawdzania spójności** wybierz sposób automatyzacji sprawdzania spójności. Można włączyć uruchamianie sprawdzania tylko wtedy, gdy dane są niespójne, lub zgodnie z harmonogramem. Jeśli nie chcesz konfigurować automatycznego sprawdzania spójności, w dowolnym momencie możesz uruchomić sprawdzanie ręczne, klikając prawym przyciskiem myszy grupę ochrony w obszarze **Ochrona** w konsoli programu DPM i wybierając polecenie **Przeprowadź sprawdzanie spójności**.
10. Jeśli wybrano opcję tworzenia kopii zapasowych w chmurze przy użyciu usługi Azure Backup, sprawdź, czy na stronie **Określanie danych chronionych w trybie online** zaznaczono obciążenia, dla których ma być tworzona kopia zapasowa na platformie Azure.
11. W obszarze **Określanie harmonogramu tworzenia kopii zapasowych online** określ, jak często mają być wykonywane przyrostowe kopie zapasowe na platformie Azure. Wykonywanie kopii zapasowych można zaplanować na każdy dzień/tydzień/miesiąc/rok, natomiast godziny/daty pozwalają ustalić konkretny czas uruchomienia wykonywania kopii zapasowych. Kopie zapasowe mogą być tworzone maksymalnie dwa razy dziennie. Zawsze podczas wykonywania kopii zapasowej na platformie Azure jest tworzony punkt odzyskiwania danych na podstawie kopii danych przechowywanych w kopii zapasowej na dysku programu DPM.
12. W polu **Określ zasady przechowywania danych online** możesz określić sposób przechowywania na platformie Azure punktów odzyskiwania tworzonych na podstawie kopii zapasowych wykonywanych co dzień/tydzień/miesiąc/rok.
13. W polu **Wybierz replikację online** określ, jak będzie wykonywana początkowa pełna replikacja danych. Możesz wykonywać replikację za pośrednictwem sieci lub tworzyć kopie zapasowe offline (rozieszczanie offline). W przypadku kopii zapasowych offline używana jest funkcja Azure Import. [Przeczytaj więcej](#).
14. Na stronie **Podsumowanie** przejrzyj ustawienia. Po kliknięciu pozycji **Utwórz grupę** następuje początkowa replikacja danych. Po ukończeniu replikacji grupa ochrony będzie mieć stan **OK** na stronie **Stan**. Następnie odbywa się tworzenie kopii zapasowych zgodnie z ustawieniami grupy ochrony.

Przygotowanie do tworzenia kopii zapasowej ogólnego źródła danych

11.12.2019 • 2 minutes to read

Program System Center Data Protection Manager (DPM) zapewnia infrastrukturę ogólnego źródła danych (GDS), dzięki czemu można chronić dowolne obciążenie firmy Microsoft, o ile ma on składnik zapisywania usługi VSS.

Oto co można zrobić:

- Pełna kopia zapasowa z użyciem ekspresowej pełnej kopii zapasowej.
- Odzyskiwanie do oryginalnej lokalizacji.
- Tworzenie kopii zapasowej referencyjnych źródeł danych.
- Tworzenie kopii zapasowej źródła danych z udostępnionymi klastrami dysków.
- Tworzenie kopii zapasowej w wielu domenach.
- Tworzenie kopii zapasowych na taśmach

Rejestrowanie nowego źródła danych

Aby dodać, usunąć lub zmodyfikować identyfikator składnika zapisywania usługi VSS dla źródła danych na liście składników zarejestrowanych w programie DPM, należy uruchomić polecenie Modify-RegisteredWriters.

Składnia

```
Modify-RegisteredWriters.ps1 [[-DpmServerName] <ciąg>] [-list] [<parametry>]
```

```
Modify-RegisteredWriters.ps1 [[-DpmServerName] <ciąg>] [-Remove] [-Writers] [<parametry>]
```

```
Modify-RegisteredWriters.ps1 [[-DpmServerName] <ciąg>] [-Add] [-Writers] [<parametry>]
```

PARAMETR	TYP	OPIS
DpmServerName	String	Określa serwer programu DPM, na którym ma zostać wykonane polecenie. Domyślnie polecenie jest wykonywane na lokalnym serwerze programu DPM.
List	SwitchParameter	Wskazuje, że polecenie powinno wyświetlić listę zarejestrowanych identyfikatorów składników zapisywania.
Dodaj	SwitchParameter	Wskazuje, że polecenie powinno dodać wprowadzone identyfikatory składników zapisywania do listy identyfikatorów składników zapisywania zarejestrowanych w programie DPM.

PARAMETR	TYP	OPIS
Usuń	SwitchParameter	Wskazuje, że należy usunąć wprowadzone identyfikatory składników zapisywania z listy identyfikatorów składników zapisywania zarejestrowanych w programie DPM.
Writers	String	Lista identyfikatorów składników zapisywania rozdzielonych przecinkami.

Przykład 1

Polecenie Modify-RegisteredWriters wyświetla listę składników zapisywania zarejestrowanych obecnie na lokalnym serwerze programu DPM.

```
Modify-RegisteredWriters -List
```

Przykład 2

Polecenie Modify-RegisteredWriters dodaje dwa nowe identyfikatory składników zapisywania do listy składników zapisywania zarejestrowanych na lokalnym serwerze programu DPM.

```
Modify-RegisteredWriters -Add -Writers "46eef637-28ca-4223-8bb6-2e87bd945179,e1cdedc6-d9d2-4fc3-8af6-5d0d0fe3e8af"
```

Przykład 3

Polecenie Modify-RegisteredWriters usuwa wskazany identyfikator składnika zapisywania z listy składników zapisywania zarejestrowanych na serwerze programu DPM dpm1.contoso.com.

```
Modify-RegisteredWriters -DpmServerName dpm1.contoso.com -Remove -Writers 46eef637-28ca-4223-8bb6-2e87bd945179
```

Przygotowywanie komputerów w grupach roboczych i domenach niezaufanych na potrzeby tworzenia kopii zapasowych

21.02.2020 • 22 minutes to read

Program System Center Data Protection Manager (DPM) może chronić komputery znajdujące się w domenach niezaufanych lub grupach roboczych. Istnieje możliwość uwierzytelniania tych komputerów za pomocą konta użytkownika lokalnego (uwierzytelnianie NTLM) lub certyfikatów. W przypadku obu typów uwierzytelniania należy przygotować infrastrukturę, zanim będzie można skonfigurować grupę ochrony zawierającą źródła, dla których chcesz utworzyć kopię zapasową.

1. **Zainstaluj certyfikat** — jeśli chcesz użyć funkcji uwierzytelniania za pomocą certyfikatu, zainstaluj certyfikat na serwerze DPM i na komputerze, który chcesz chronić.
2. **Zainstaluj agenta** — zainstaluj agenta ochrony na komputerze, który chcesz chronić.
3. **Rozpoznaj serwer DPM** — skonfiguruj komputer tak, aby rozpoznawał serwer DPM w celu umożliwienia tworzenia kopii zapasowych. W tym celu należy uruchomić polecenie SetDPMServer.
4. **Dołącz komputer** — w ostatnim kroku dołącz komputer chroniony do serwera DPM.

Przed rozpoczęciem

Przed rozpoczęciem Sprawdź Obsługiwane scenariusze ochrony i wymagane ustawienia sieci.

Scenariusze obsługiwane

TYP OBCIĄŻEŃ	STAN I POMOC TECHNICZNA SERWERA CHRONIONEGO
Pliki	Grupa robocza: Obsługiwane Domena niezaufana: obsługiwane Uwierzytelnianie NTLM i uwierzytelnianie certyfikatu na jednym serwerze. Uwierzytelnianie certyfikatu tylko dla klastra.
Stan systemu	Grupa robocza: Obsługiwane Domena niezaufana: obsługiwane Tylko uwierzytelnianie NTLM
Serwer SQL	Grupa robocza: Obsługiwane Domena niezaufana: obsługiwane Dublowanie nie jest obsługiwane. Uwierzytelnianie NTLM i uwierzytelnianie certyfikatu na jednym serwerze. Uwierzytelnianie certyfikatu tylko dla klastra.

TYP OBCIĄŻEŃ	STAN I POMOC TECHNICZNA SERWERA CHRONIONEGO
Serwer funkcji Hyper-V	Grupa robocza: Obsługiwane Domena niezaufana: obsługiwane Uwierzytelnianie NTLM i uwierzytelnianie certyfikatu
Klaster Hyper-V	Grupa robocza: Nieobsługiwane Domena niezaufana: obsługiwane (tylko uwierzytelnianie certyfikatów)
Exchange Server	Grupa robocza: Nie dotyczy Domena niezaufana: obsługiwane tylko w przypadku jednego serwera. Klaster nie jest obsługiwany. Formaty CCR, SCR i DAG nie są obsługiwane. Usługa LCR jest obsługiwana. Tylko uwierzytelnianie NTLM
Pomocniczy serwer programu DPM (do tworzenia kopii zapasowej podstawowego serwera programu DPM) Uwaga: Zarówno podstawowy, jak i pomocniczy serwer programu DPM muszą znajdować się w tej samej lub zaufanej domenie.	Grupa robocza: Obsługiwane Domena niezaufana: obsługiwane Tylko uwierzytelnianie certyfikatu
SharePoint	Grupa robocza: Nieobsługiwane Domena niezaufana: nieobsługiwane
Komputery klienckie	Grupa robocza: Nieobsługiwane Domena niezaufana: nieobsługiwane
Odzyskiwanie systemu od zera (BMR)	Grupa robocza: Nieobsługiwane Domena niezaufana: nieobsługiwane
Odzyskiwanie przez użytkownika końcowego	Grupa robocza: Nieobsługiwane Domena niezaufana: nieobsługiwane

Ustawienia sieciowe

USTAWIENIA	KOMPUTER W GRUPIE ROBOCZEJ LUB W NIEZAUFANEJ DOMENIE
dane kontrolne	Protokół: DCOM Port domyślny: 135 Uwierzytelnianie: NTLM/certyfikat
Transfer plików	Protokół: Winsock Port domyślny: 5718 i 5719 Uwierzytelnianie: NTLM/certyfikat

USTAWIENIA	KOMPUTER W GRUPIE ROBOCZEJ LUB W NIEZAUFANEJ DOMENIE
Wymagania konta programu DPM	Konto lokalne bez uprawnień administratora na serwerze DPM. Wykorzystuje komunikację NTLM v2
Wymagania certyfikatu	
Instalacja agenta	Agent zainstalowany na komputerze chronionym
Sieć obwodowa	Ochrona sieci obwodowej nie jest obsługiwana.
IPSEC	Upewnij się, że protokół IPSEC nie blokuje komunikacji.

Tworzenie kopii zapasowej przy użyciu uwierzytelniania NTLM

Oto czynności, jakie należy wykonać:

1. Zainstaluj agenta — zainstaluj agenta ochrony na komputerze, który chcesz chronić.
2. Skonfiguruj agenta — skonfiguruj komputer tak, aby rozpoznawał serwer DPM podczas tworzenia kopii zapasowych. W tym celu należy uruchomić polecenie SetDPMServer.
3. Dołącz komputer — w ostatnim kroku dołącz komputer chroniony do serwera DPM.

Instalowanie i konfigurowanie agenta

1. Na komputerze, który ma być chroniony, uruchom program DPMAgentInstaller_X64.exe z instalacyjnego dysku CD programu DPM, aby zainstalować agenta.
2. Skonfiguruj agenta, uruchamiając następujące polecenie SetDpmServer:

```
SetDpmServer.exe -dpmServerName <serverName> -isNonDomainServer -userName <userName> [-productionServerDnsSuffix <DnsSuffix>]
```

3. Określ wartości następujących parametrów:

- **-DpmServerName** — określ nazwę serwera DPM. Użyj nazwy FQDN, jeśli serwer i komputer mogą uzyskiwać wzajemny dostęp przy użyciu nazw FQDN, lub nazwy NETBIOS.
- **-IsNonDomainServer** — użyj tego parametru, aby wskazać, że serwer należy do grupy roboczej lub niezaufanej domeny powiązanej z komputerem, który chcesz chronić. Dla wymaganych portów tworzone są wyjątki zapory.
- **-UserName** — określ nazwę konta do użycia na potrzeby uwierzytelniania NTLM. Aby korzystanie z tej opcji było możliwe, należy określić flagę -isNonDomainServer. Zostanie utworzone konto użytkownika lokalnego, a agent ochrony programu DPM zostanie skonfigurowany do korzystania z tego konta w ramach uwierzytelniania.
- **-ProductionServerDnsSuffix** — użyj tego przełącznika, jeśli skonfigurowano wiele sufiksów DNS serwera. Ten przełącznik reprezentuje sufiks DNS używany na serwerze do nawiązywania połączenia z komputerem chronionym.

4. Po pomyślnym zakończeniu działania polecenia otwórz konsolę programu DPM.

Aktualizowanie hasła

Aby w dowolnym momencie zaktualizować hasło dla poświadczeń NTLM, uruchom następujące polecenie na komputerze chronionym:

```
SetDpmServer.exe -dpmServerName <serverName> -isNonDomainServer -updatePassword
```

Użyj tej samej konwencji nazewnictwa (FQDN lub NETBIOS), która została zastosowana podczas konfigurowania ochrony. Na serwerze DPM uruchom polecenie cmdlet programu PowerShell Update -NonDomainServerInfo. Następnie odśwież informacje agenta dla komputera chronionego.

Przykład nazwy NetBIOS: Komputer chroniony:

```
SetDpmServer.exe -dpmServerName Server01 -isNonDomainServer -UpdatePassword
```

 Serwer DPM:

```
Update-NonDomainServerInfo -PSName Finance01 -dpmServerName Server01
```

Przykład nazwy FQDN: Komputer chroniony:

```
SetDpmServer.exe -dpmServerName Server01.corp.contoso.com -isNonDomainServer -UpdatePassword
```

 Serwer DPM:

```
Update-NonDomainServerInfo -PSName Finance01.worldwideimporters.com -dpmServerName Server01.contoso.com
```

Dołączanie komputera

1. W konsoli programu DPM uruchom kreatora instalacji agenta ochrony.
2. W oknie **Wybierz metodę wdrożenia agenta** wybierz opcję **Przyłącz agentów**.
3. Wprowadź nazwę komputera, nazwę użytkownika i hasło dla docelowego komputera dołączania. Powinny być to poświadczenia określone podczas instalacji agenta.
4. Zapoznaj się z informacjami na stronie **Podsumowanie** i kliknij pozycję **Dołącz**.

Opcjonalnie — zamiast uruchamiania kreatora — możesz uruchomić polecenie programu Windows PowerShell Attach-NonDomainServer.ps1. Aby to zrobić, zapoznaj się z przykładem w następnej sekcji.

Przykłady

Przykład 1

Przykład konfigurowania komputera grupy roboczej po zainstalowaniu agenta.

1. Na komputerze uruchom polecenie

```
SetDpmServer.exe -DpmServerName Server01 -isNonDomainServer -UserName mark .
```

2. Na serwerze DPM uruchom polecenie

```
Attach-NonDomainServer.ps1 -DpmServername Server01 -PSName Finance01 -Username mark .
```

Ze względu na to, że komputery grupy roboczej są zazwyczaj dostępne tylko przy użyciu nazwy NetBIOS, wartość parametru DPMServerName musi być nazwą NetBIOS.

Przykład 2

Przykład konfigurowania komputera grupy roboczej z nazwami NetBIOS powodującymi konflikt po zainstalowaniu agenta.

1. Na komputerze grupy roboczej uruchom polecenie

```
SetDpmServer.exe -dpmServerName Server01.corp.contoso.com -isNonDomainServer -userName mark -  
productionServerDnsSuffix widgets.corp.com
```

.

2. Na serwerze DPM uruchom polecenie

```
Attach-NonDomainServer.ps1 -DPMServername Server01.corp.contoso.com -PSName Finance01.widgets.corp.com -  
Username mark
```

.

Tworzenie kopii zapasowej przy użyciu uwierzytelniania za pomocą

certyfikatu

Oto instrukcje konfigurowania ochrony z uwierzytelnianiem za pomocą certyfikatu.

- Na każdym komputerze, który ma być chroniony, musi być zainstalowane oprogramowanie .NET Framework w wersji co najmniej 3.5 z dodatkiem SP1.
- Certyfikat używany do uwierzytelniania musi spełniać następujące warunki:
 - Certyfikat X.509 V3
 - Rozszerzone użycie klucza (EKU) powinno obejmować uwierzytelnianie klienta i serwera.
 - Długość klucza powinna wynosić co najmniej 1024 bity.
 - Typem klucza musi być **exchange**.
 - Nazwa podmiotu certyfikatu i certyfikat główny nie mogą być puste.
 - Serwery odwołań powiązanych urzędów certyfikacji muszą być online i dostępne zarówno dla chronionego serwera, jak i serwera DPM.
 - Z certyfikatem musi być powiązany klucz prywatny.
 - Program DPM nie obsługuje certyfikatów z kluczami CNG
 - Program DPM nie obsługuje certyfikatów z podpisem własnym.
- Każdy komputer, który ma być chroniony (w tym maszyny wirtualne), musi mieć własny certyfikat.

Konfigurowanie ochrony

1. [Tworzenie szablonu certyfikatu programu DPM](#)
2. [Konfigurowanie certyfikatu na serwerze DPM](#).
3. [Instalowanie agenta](#)
4. [Konfigurowanie certyfikatu na chronionym komputerze](#)
5. [Dołączanie komputera](#)

Tworzenie szablonu certyfikatu programu DPM

Opcjonalnie możesz skonfigurować szablon programu DPM na potrzeby rejestracji w sieci Web. Jeśli chcesz to zrobić, wybierz szablon, którego zamierzony cel to Uwierzytelnianie klienta i Uwierzytelnianie serwera. Przykład:

1. W przystawce MMC **Szablony certyfikatów** możesz wybrać szablon **Serwery RAS i IAS**. Kliknij go prawym przyciskiem myszy i wybierz polecenie **Duplikuj szablon**.
2. W oknie **Duplikowanie szablonu** pozostaw domyślne ustawienie **Windows Server 2003 Enterprise**.
3. Na karcie **Ogólne** zmień nazwę wyświetlaną szablonu na mówiącą coś o nim. Na przykład **Uwierzytelnianie DPM**. Upewnij się, że włączone jest ustawienie **Publikuj certyfikat w usłudze Active Directory**.
4. Na karcie **Obsługiwanie żądań** upewnij się, że włączone jest ustawienie **Zezwalaj na eksportowanie klucza prywatnego**.
5. Po utworzeniu szablonu zezwól na jego używanie. Otwórz przystawkę Urząd certyfikacji. Kliknij prawym przyciskiem myszy pozycję **Szablony certyfikatów**, wybierz polecenie **Nowy**, a następnie **Szablon certyfikatu do wystawienia**. W oknie **Włączanie szablonu certyfikatu** wybierz szablon i kliknij przycisk OK. Teraz szablon będzie dostępny podczas uzyskiwania certyfikatu.

Włączanie rejestrowania lub autorejestrowania

Jeśli chcesz opcjonalnie skonfigurować szablon na potrzeby rejestrowania lub autorejestrowania, kliknij kartę **Nazwa podmiotu** we właściwościach szablonu. Po skonfigurowaniu rejestrowania szablon można wybrać w przystawce MMC. Jeśli zostanie skonfigurowane autorejestrowanie, certyfikat zostanie automatycznie przypisany do wszystkich komputerów w domenie.

- Na czas rejestrowania na karcie **Nazwa podmiotu** we właściwościach szablonu włącz ustawienie **Konstruuje z tej informacji usługi Active Directory**. W polu **Format nazwy podmiotu** wybierz opcję **Nazwa pospolita** i włącz ustawienie **Nazwa DNS**. Następnie przejdź na kartę **Zabezpieczenia** i przyznaj uprawnienie **Rejestrowanie** użytkownikom uwierzytelnionym.
- W przypadku autorejestrowania przejdź na kartę **Zabezpieczenia** i przyznaj uprawnienie **Autorejestrowanie** użytkownikom uwierzytelnionym. Po włączeniu tego ustawienia certyfikat zostanie automatycznie przypisany do wszystkich komputerów w domenie.
- Jeśli skonfigurowano rejestrowanie, w przystawce MMC będzie można wprowadzać żądania nowego certyfikatu na podstawie szablonu. Aby to zrobić, na chronionym komputerze w sekcji **Certyfikaty (komputer lokalny)** > **Osobiste** kliknij prawym przyciskiem myszy pozycję **Certyfikaty**. Wybierz polecenie **Wszystkie zadania** > **Żądaj nowego certyfikatu**. Na stronie **Wybierz zasady rejestracji certyfikatu** kreatora wybierz opcję **Zasady rejestracji usługi Active Directory**. W oknie **Żądaj certyfikatów** będzie widoczny szablon. Rozwiń węzeł **Szczegóły** i kliknij polecenie **Właściwości**. Wybierz kartę **Ogólne** i podaj przyjazną nazwę. Po zastosowaniu ustawień powinien zostać wyświetlony komunikat o pomyślnym zarejestrowaniu certyfikatu.

Konfigurowanie certyfikatu na serwerze DPM

1. Wygeneruj certyfikat z urzędu certyfikacji dla serwera DPM za pomocą rejestracji w sieci Web lub innej metody. W przypadku rejestracji w sieci Web wybierz opcję **zaawansowane żądanie certyfikatu** oraz **Utwórz i prześlij żądanie do tego urzędu certyfikacji**. Upewnij się, że rozmiar klucza wynosi co najmniej 1024 i wybrana jest opcja **Oznacz ten klucz jako eksportowalny**.
2. Certyfikat zostanie umieszczony w magazynie Użytkownik. Trzeba przenieść go do magazynu Komputer lokalny.
3. W tym celu należy wyeksportować certyfikat z magazynu użytkownika. Certyfikat trzeba wyeksportować razem z kluczem prywatnym. Możesz wyeksportować go w domyślnym formacie pfx. Podaj hasło do eksportowanego pliku.
4. W obszarze Komputer lokalny\Osobiste\Certyfikat uruchom Kreatora importu certyfikatów, aby zaimportować wyeksportowany plik z miejsca, w którym został zapisany. Podaj hasło użyte podczas eksportowania i upewnij się, że włączona jest opcja **Oznacz ten klucz jako eksportowalny**. Na stronie Magazyn certyfikatów pozostaw domyślne ustawienie **Umieść wszystkie certyfikaty w następującym magazynie** i upewnij się, że wybrana jest opcja **Osobiste**.
5. Po zaimportowaniu ustaw używanie certyfikatu jako poświadczeń programu DPM w następujący sposób:
 - a. Uzyskaj odcisk palca certyfikatu. W magazynie **Certyfikaty** kliknij dwukrotnie certyfikat. Wybierz kartę **Szczegóły** i przewiń w dół do odcisku palca. Kliknij go, zaznacz i skopiuj. Wklej odcisk palca do Notatnika i usuń wszystkie spacje.
 - b. Uruchom polecenie **Set-DPMCredentials**, aby skonfigurować serwer DPM:

```
Set-DPMCredentials [-DPMServerName <String>] [-Type <AuthenticationType>] [Action <Action>] [-OutputFilePath <String>] [-Thumbprint <String>] [-AuthCAThumbprint <String>]
```

- **-Type** — wskazuje typ uwierzytelniania. Wartość: **certificate**.
- **-Action** — wskazuje, czy polecenie ma zostać wykonane po raz pierwszy, czy poświadczenia mają

zostać wygenerowane ponownie. Dopuszczalne wartości: **regenerate** (generuj ponownie) lub **configure** (konfiguruj).

- **-OutputFilePath** — lokalizacja pliku wyjściowego używanego w poleceniu Set-DPMsServer na komputerze chronionym.
 - **-Thumbprint** — skopiuj z Notatnika.
 - **-AuthCATthumbprint** — odcisk palca urzędu certyfikacji w łańcuchu zaufania certyfikatu. Opcjonalny. Jeśli nie jest podany, zostanie użyty urząd główny.
6. Uruchomienie tego polecenia spowoduje wygenerowanie pliku metadanych (bin) wymaganego podczas każdego instalowania agenta w niezaufanej domenie. Przed uruchomieniem polecenia musi istnieć folder C:\Temp. Jeśli plik zostanie utracony lub usunięty, można go utworzyć ponownie przez uruchomienie skryptu z opcją **-action regenerate**.
 7. Skopiuj plik bin do folderu C:\Program Files\Microsoft Data Protection Manager\DPM\bin na komputerze, który ma być chroniony. Nie jest to konieczne, ale jeśli tego nie zrobisz, musisz podać pełną ścieżkę do tego pliku w parametrze -DPMcredential podczas
 8. Powtórz te czynności na każdym serwerze DPM chroniącym komputery w grupie roboczej lub niezaufanej domenie.

Instalowanie agenta

1. Na każdym komputerze, który ma być chroniony, uruchom program DPMAgentInstaller_X64.exe z instalacyjnej płyty CD programu DPM, aby zainstalować agenta.

Konfigurowanie certyfikatu na chronionym komputerze

1. Wygeneruj certyfikat z urzędu certyfikacji dla chronionego komputera za pomocą rejestrowania w sieci Web lub innej metody. W przypadku rejestracji w sieci Web wybierz opcje **zaawansowane żądanie certyfikatu** oraz **Utwórz i prześlij żądanie do tego urzędu certyfikacji**. Upewnij się, że rozmiar klucza wynosi co najmniej 1024 i wybrana jest opcja **Oznacz ten klucz jako eksportowalny**.
2. Certyfikat zostanie umieszczony w magazynie Użytkownik. Trzeba przenieść go do magazynu Komputer lokalny.
3. W tym celu należy wyeksportować certyfikat z magazynu użytkownika. Certyfikat trzeba wyeksportować razem z kluczem prywatnym. Możesz wyeksportować go w domyślnym formacie pfx. Podaj hasło do eksportowanego pliku.
4. W obszarze Komputer lokalny\Osobiste\Certyfikat uruchom Kreatora importu certyfikatów, aby zaimportować wyeksportowany plik z miejsca, w którym został zapisany. Podaj hasło użyte podczas eksportowania i upewnij się, że włączona jest opcja **Oznacz ten klucz jako eksportowalny**. Na stronie Magazyn certyfikatów pozostaw domyślne ustawienie **Umieść wszystkie certyfikaty w następującym magazynie** i upewnij się, że wybrana jest opcja **Osobiste**.
5. Po zaimportowaniu skonfiguruj na komputerze rozpoznawanie serwera DPM jako autoryzowanego do wykonywania kopii zapasowych w następujący sposób
 - a. Uzyskaj odcisk palca certyfikatu. W magazynie **Certyfikaty** kliknij dwukrotnie certyfikat. Wybierz kartę **Szczegóły** i przewiń w dół do odcisku palca. Kliknij go, zaznacz i skopiuj. Wklej odcisk palca do Notatnika i usuń wszystkie spacje.
 - b. Przejdź do folderu C:\Program files\Microsoft Data Protection Manager\DPM\bin. Następnie uruchom polecenie **setdpmserver** w poniższy sposób:

```
setdpmserver -dpmCredential CertificateConfiguration_DPM01.contoso.com.bin -OutputFilePath  
c:\Temp -Thumbprint <ClientThumbprintWithNoSpaces
```

Gdzie odcisk palca ClientThumbprintWithNoSpaces jest skopiowany z pliku w Notatniku.

- c. Powinien zostać wyświetlony komunikat potwierdzający pomyślne przeprowadzenie konfiguracji.
6. Skopiuj plik bin na serwer DPM. Sugerujemy skopiowanie go do lokalizacji domyślnej, w której będzie go szukać proces Attach (Windows\System32), dzięki czemu podczas uruchamiania polecenia Attach wystarczy podać samą nazwę pliku zamiast pełnej ścieżki.

Dołączanie komputera

Aby dołączyć komputer do serwera DPM, użyj skryptu PowerShell Attach-ProductionServerWithCertificate.ps1 z poniższymi parametrami.

```
Attach-ProductionServerWithCertificate.ps1 [-DPMServerName <String>] [-PSCredential <String>]  
[<CommonParameters>]
```

- -DPMServerName — nazwa serwera DPM,
- PSCredential — nazwa pliku bin. Jeśli plik został skopiowany do folderu Windows\System32, wystarczy podać tylko jego nazwę. Należy zachować ostrożność, aby określić plik bin utworzony na chronionym serwerze. Jeśli wskażesz plik bin utworzony na serwerze DPM, usuniesz wszystkie chronione komputery, które mają skonfigurowane uwierzytelnianie na podstawie certyfikatów.

Po zakończeniu procesu dołączania komputer chroniony powinien być widoczny w konsoli programu DPM.

Przykłady

Przykład 1

Wygenerowanie w folderze `c:\CertMetaData\` pliku o nazwie `CertificateConfiguration\_<DPM SERVER FQDN>.bin`

```
Set-DPMCredentials -DPMServerName dpmserver.contoso.com -Type Certificate -Action Configure -OutputFilePath  
c:\CertMetaData\ -Thumbprint "cf822d9ba1c801ef40d4b31de0cfcb200a8a2496"
```

Gdzie dpmserver.contoso.com jest nazwą serwera DPM, a „cf822d9ba1c801ef40d4b31de0cfcb200a8a2496” to odcisk palca certyfikatu serwera DPM.

Przykład 2

Ponowne wygenerowanie utraconego pliku konfiguracji w folderze `c:\CertMetaData\`

```
Set-DPMCredentials -DPMServerName dpmserver.contoso.com -Type Certificate "-OutputFilePath c:\CertMetaData\ -  
Action Regenerate
```

Tworzenie kopii zapasowej serwera DPM

11.12.2019 • 62 minutes to read

Aby zapewnić, że dane mogą zostać odzyskane, jeśli program System Center Data Protection Manager (DPM) ulegnie awarii, potrzebna będzie strategia tworzenia kopii zapasowej serwera programu DPM. Jeśli kopie zapasowe nie są tworzone, po awarii trzeba odbudować dane ręcznie, a punktów odzyskiwania na dysku nie da się odzyskać. Kopię zapasową serwerów DPM można utworzyć przy użyciu kilku metod:

- **Tworzenie kopii zapasowej serwera programu DPM** — można utworzyć kopię zapasową podstawowego serwera DPM przy użyciu pomocniczego serwera DPM. Serwer pomocniczy będzie chronić bazę danych serwera podstawowego i repliki źródła danych przechowywane na serwerze podstawowym. W razie awarii serwera podstawowego serwer pomocniczy może nadal chronić obciążenia chronione przez serwer podstawowy do czasu, aż serwer podstawowy stanie się ponownie dostępny. W razie potrzeby odbudowania serwera podstawowego można przywrócić bazy danych i repliki z serwera pomocniczego. Gdy serwer podstawowy jest niedostępny, dane można przywrócić na chronione komputery bezpośrednio z serwera pomocniczego. Można skonfigurować dwa serwery, jeden jako podstawowy, a drugi jako pomocniczy, lub skonfigurować oba serwery, aby działały dla siebie wzajemnie jako podstawowe. Można również skonfigurować łańcuch serwerów DPM, chroniących się wzajemnie zgodnie z kolejnością łańcucha.
- **Tworzenie kopii zapasowej bazy danych programu DPM** — można skonfigurować serwer programu DPM, aby tworzył kopie zapasowe własnych baz danych w bibliotece taśm, lub użyć oprogramowania firmy innej niż Microsoft do wykonania kopii zapasowej baz danych na taśmie lub nośnikach wymiennych.
- **Tworzenie kopii zapasowej programu DPM przy użyciu oprogramowania innej firmy** — można utworzyć kopię zapasową serwerów DPM za pomocą oprogramowania innych firm, które obsługuje program DPM i technologię VSS.

Tworzenie kopii zapasowej za pomocą pomocniczego serwera programu DPM

Można utworzyć kopie zapasowe informacji znajdujących się na serwerze programu DPM oraz chronić je przy użyciu innego serwera programu DPM w jednej z następujących konfiguracji:

- **Ochrona podstawowa i pomocnicza** — można utworzyć kopie zapasowe bazy danych i replik przechowywanych na podstawowym serwerze programu DPM na pomocniczym serwerze programu DPM. Jeśli serwer podstawowy ulegnie awarii, serwer pomocniczy nadal tworzy kopie zapasowe chronionych obciążeń. Jeśli awarii ulegnie serwer podstawowy, możesz wykonać jedną z następujących czynności: Odbuduj serwer podstawowy i przywróć jego bazę danych i repliki z serwera pomocniczego. Następnie po odbudowaniu przenieś chronione obciążenia z powrotem na serwer podstawowy. Wybierz opcję przełączenia ochrony na pomocniczy serwer DPM. To ustawienie umożliwia przywrócenie komputera chronionego bezpośrednio z serwera pomocniczego, jeśli zaistnieje taka potrzeba. Instrukcje można znaleźć w artykule Konfigurowanie serwerów pomocniczych.
- **Łańcuch serwerów programu DPM** — łańcuch serwerów DPM zapewnia ochronę i każdy z serwerów chroni kolejny serwer w łańcuchu. Na przykład: Serwer DPM1 jest chroniony przez serwer DPM2 (DPM1 jest serwerem podstawowym, a DPM2 pomocniczym). DPM2 jest chroniony przez DPM3 (DPM2 jest podstawowym, a DPM3 jest pomocniczą) do instrukcji, zobacz Konfigurowanie łańcucha.
- **Ochrona cykliczna** — jeden serwer DPM tworzy kopie zapasowe innego serwera DPM i na odwrót. Tak więc serwer DPM1 chroni serwer DPM2, a serwer DPM2 chroni serwer DPM1. Jest to przydatne w przypadku małych środowisk.

Konfigurowanie ochrony podstawowej i pomocniczej

Utwórz kopię zapasową głównego serwera programu DPM za pomocą serwera pomocniczego:

1. Zainstaluj agenta ochrony programu DPM na każdym podstawowym serwerze programu DPM, który chcesz chronić. Nie jest wymagane ponowne uruchomienie.

IMPORTANT

Wersje główne i pomocnicze podstawowych i pomocniczych serwerów programu DPM muszą być zgodne.

2. Dodaj podstawowy serwer programu DPM do istniejącej grupy ochrony lub utwórz nową. Wybierz do ochrony następujące źródła danych:

- bazy danych programu SQL Server skonfigurowane dla serwera podstawowego;
- wszystkie woluminy na serwerze głównym programu DPM (udziały nie będą wyświetlane osobno);
- wszystkie repliki na serwerze głównym programu DPM.
- Należy wybrać co najmniej te bazy danych, pliki programu \program\Microsoft System Center\DPM\programu DPM\folder konfiguracyjny i \pliki programu\programu Microsoft System Center\DPM\Scripting.

Pamiętaj, że z ochrony repliki nie można wykluczyć rozszerzeń nazw plików. Ponadto wszystkie serwery DPM muszą mieć uruchomioną tę samą wersję, aktualizacje itp. Podczas konfigurowania synchronizacji zalecamy synchronizację co 24 godziny.

Konfigurowanie łańcucha serwerów programu DPM

Zanim zaczniesz rozważać utworzenie łańcuch, weź pod uwagę następujące ograniczenia:

- Każdy serwer programu DPM może być chroniony tylko raz w łańcuchu, dlatego należy sprawdzić, czy nie jest chroniony przez więcej niż jeden serwer.
- Serwery podstawowe i pomocnicze są ustanowione przez strukturę łańcucha. Tak więc, na przykład, jeśli serwer DPM3 faktycznie chroni serwer DPM1, ponieważ działa jako pomocniczy serwer dla DPM2, nie może działać bezpośrednio jako serwer pomocniczy dla DPM1.
- Jeśli serwer DPM zostanie skonfigurowany tak, aby chronić swoje własne źródło danych, łańcuch zostanie przerwany. Na przykład jeśli DPM1 chroni własną bazę danych lub stan systemu, DPM2 nie może chronić DPM1.
- Przed rozpoczęciem ochrony bazy danych podstawowego serwera DPM należy na tym serwerze podstawowym uruchomić usługę składnika zapisywania usługi VSS programu SQL Server.

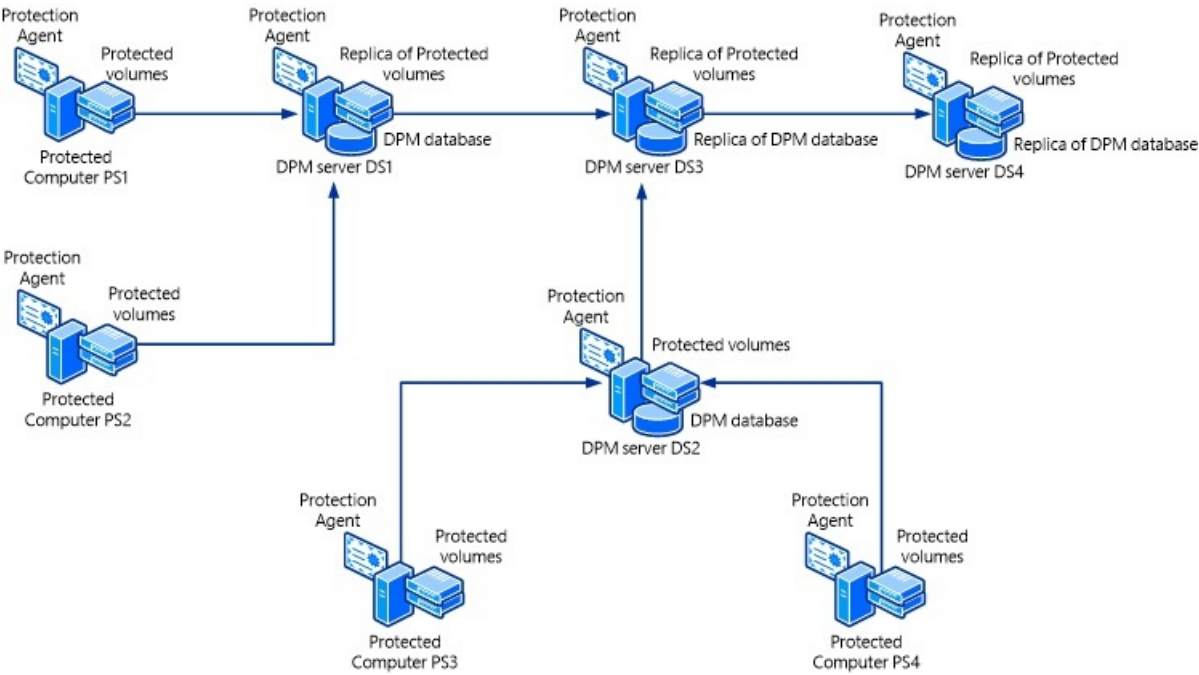
Przykładowy łańcuch 1

Scenariusz 1: ochrona łańcuchowa

W scenariuszu 1 łańcuch jest tworzony przez cztery serwery programu DPM:

SERWER	CHRONI	CHRONIONY PRZEZ
DS1 (podstawowy)	PS1, PS2	DS3
DS2 (podstawowy)	PS3, PS4	DS3
DS3 (pomocniczy)	DS1, DS2	DS4

SERWER	CHRONI	CHRONIONY PRZEZ
DS4 (pomocniczy)	DS3	-

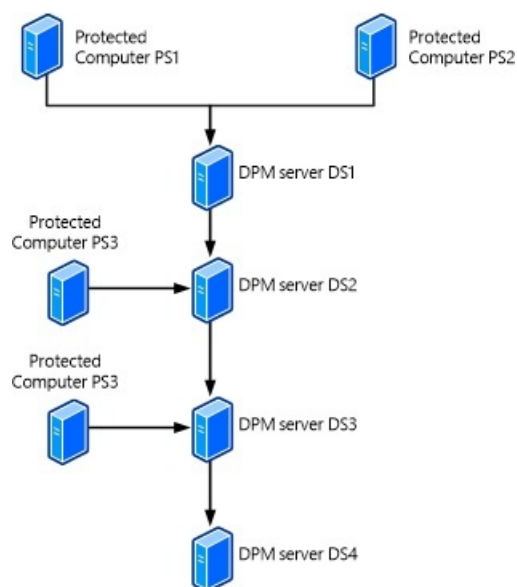


Przykładowy łańcuch 2

Scenariusz 2: ochrona łańcuchowa

W scenariuszu 2 łańcuch jest tworzony przez cztery serwery programu DPM:

SERWER	CHRONI	CHRONIONY PRZEZ
DS1 (podstawowy)	PS1, PS2	DS2
DS2 (podstawowy)	PS3	DS3
DS2 (pomocniczy)	DS1	DS3
DS3 (podstawowy)	PS4	DS4
DS3 (pomocniczy)	DS2	DS4
DS4	DS3	-



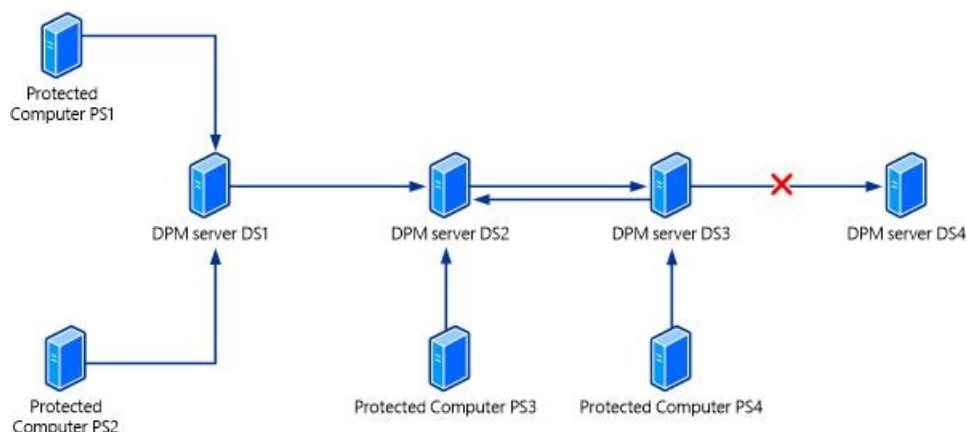
Ochrona cykliczna

Jeśli nie chcesz używać serwera pomocniczego, dwa serwery programu DPM mogą chronić siebie nawzajem.

Scenariusz 3: ochrona cykliczna

W scenariuszu 3 przedstawiono ochronę cykliczną.

SERWER	CHRONI	CHRONIONY PRZEZ
DS1 (podstawowy)	PS1, PS2	DS2
DS2 (podstawowy)	PS3	DS3
DS2 (pomocniczy)	DS1, DS3	DS3
DS3 (podstawowy)	PS4	DS2
DS3 (pomocniczy)	DS2	DS2



Konfigurowanie łańcucha

Skonfiguruj łańcuch w następujący sposób:

1. Zainstaluj agenta ochrony programu DPM na serwerze programu DPM, który ma być chroniony, używając serwera programu DPM, który ma go chronić.
2. Skonfiguruj dodatkową ochronę dla źródeł danych chronionych przez serwer programu DPM, który chronisz. Zwróć uwagę, że w konsoli programu DPM nie można skonfigurować ochrony źródeł danych,

które są już chronione przez agenta. Zapobiega to wielokrotnej ochronie danych.

3. Na przykład mając serwery DPM1 i DPM2, możesz zainstalować agenta ochrony programu DPM z serwera DPM1 na serwerze DPM2 i na odwrót. Następnie skonfiguruj ochronę pomocniczą na serwerze DPM2 dla serwerów, które są chronione przez serwer DPM1, i ochronę pomocniczą na serwerze DPM1 dla serwerów, które są chronione przez serwer DPM2.

Odzyskiwanie serwera

Jeśli serwer podstawowy ulegnie awarii, można przełączyć ochronę na serwer pomocniczy. Po przełączeniu ochrony można wykonywać funkcje odzyskiwania z serwera pomocniczego.

- Aby przełączyć ochronę na serwer pomocniczy, w konsoli programu DPM kliknij prawym przyciskiem myszy grupę ochrony, dla której chcesz przełączyć ochronę, a następnie wybierz polecenie **Przełączyć ochronę przed awarią**. Replika będzie wyglądała na niespójną, dopóki nie zostanie uruchomione sprawdzanie spójności.
- W przypadku odzyskiwania podstawowego serwera programu DPM musisz ponownie ustawić ochronę komputerów, które były wcześniej chronione za pomocą tego serwera. Pamiętaj, że nie możesz przywracać punktów odzyskiwania, a po przywróceniu plików bazy danych musisz upewnić się, że lokalizacja przywracania na serwerze programu DPM jest bezpieczna.

Musisz odzyskać bazę danych programu DPM, a następnie wszystkie repliki.

- Następnie ustanów ponownie ochronę, uruchamiając plik Setdpmserver.exe.

Tworzenie kopii zapasowej bazy danych programu DPM

W ramach strategii tworzenia kopii zapasowych programu DPM musisz wykonać kopię zapasową bazy danych programu DPM. Baza danych programu DPM nosi nazwę DPMDB. Ta baza danych zawiera konfigurację programu DPM oraz dane dotyczące jego kopii zapasowych. W razie awarii z jej ostatniej kopii zapasowej można odtworzyć większość funkcjonalności serwera DPM. Przy założeniu, że można przywrócić bazę danych, kopie zapasowe na taśmach są dostępne, a wszystkie ustawienia grup ochrony i harmonogramy kopii zapasowych zostaną zachowane. O ile awaria nie wpłynęła na dyski puli magazynów programu DPM, również kopie zapasowe na dyskach będą nadawały się do użycia po odbudowie. Istnieje kilka różnych metod wykonywania kopii zapasowych bazy danych.

METODA TWORZENIA KOPII ZAPASOWEJ BAZY DANYCH	ZALETY	WADY
--	--------	------

METODA TWORZENIA KOPII ZAPASOWEJ BAZY DANYCH	ZALETY	WADY
Tworzenie kopii zapasowej na platformie Azure	Łatwa konfiguracja i monitorowanie w programie DPM. Wiele lokalizacji plików kopii zapasowej bazy danych. Magazyn w chmurze zapewnia niezawodne rozwiązanie odzyskiwania po awarii. Bardzo bezpieczny magazyn na bazę danych. Obsługuje 120 punktów odzyskiwania online.	Dostępna tylko w programie DPM 2012 z dodatkiem SP1 lub nowszym. Wymaga konta systemu Azure i dodatkowej konfiguracji programu DPM. Generuje pewien koszt związany z magazynem systemu Azure. Aby uzyskać dostęp do kopii zapasowych programu DPM przechowywanych w magazynie kopii zapasowych platformy Azure, - wymaga obsługiwanej wersji systemu Windows Server z usługą Azure Agent. Nie może to być inny serwer DPM. Opcja ta nie jest możliwa, jeśli baza danych jest przechowywana lokalnie i chcesz włączyć dodatkową ochronę. Obejściem byłoby użycie bazy danych na zdalnym serwerze SQL Server. Wymaga pewnego dodatkowego czasu na przygotowanie i odzyskiwanie.
Tworzenie kopii zapasowej bazy danych przez utworzenie kopii zapasowej puli magazynów programu DPM	Prosta do konfigurowania i monitorowania. Kopia zapasowa jest przechowywana na dyskach puli magazynów programu DPM i łatwo uzyskać do niej dostęp lokalnie. Zaplanowane kopie zapasowe programu DPM obsługują 512 ekspresowych pełnych kopii zapasowych. W przypadku tworzenia kopii zapasowej co godzinę masz 21 dni pełnej ochrony.	Nie jest to dobra opcja w przypadku odzyskiwania po awarii. Działa w trybie online, a odzyskiwanie może nie przebiegać zgodnie z oczekiwaniami, jeśli serwer DPM lub dysk puli magazynów ulegnie awarii. Opcja ta nie jest możliwa, jeśli baza danych jest przechowywana lokalnie i chcesz włączyć dodatkową ochronę. Obejściem byłoby użycie bazy danych na zdalnym serwerze SQL Server. Jeśli usługa DPM lub konsola nie uruchamia się lub nie działa, konieczne są pewne przygotowania i specjalne kroki w celu uzyskania dostępu do punktów odzyskiwania.

METODA TWORZENIA KOPII ZAPASOWEJ BAZY DANYCH	ZALETY	WADY
Tworzenie kopii zapasowej na pomocniczym serwerze DPM	Łatwa konfiguracja i monitorowanie w programie DPM. Zaplanowane kopie zapasowe programu DPM obsługują 512 ekspresowych pełnych kopii zapasowych. W przypadku wykonywania co godzinę umożliwią 21 dni ochrony krótkoterminowej. Jeśli będą wykonywane co 30 minut, zapewnią ochronę 10-dniową. Kopia zapasowa jest przechowywana na dyskach puli magazynów pomocniczego serwera DPM, które są dostępne lokalnie. Zapewnia dobre rozwiązanie odzyskiwania po awarii, jeśli pomocniczy serwer DPM znajduje się poza siedzibą firmy.	Wymaga dodatkowego serwera DPM i magazynu. Oba serwery DPM muszą mieć tę samą wersję programu DPM i te same pakiety zbiorcze aktualizacji.
Tworzenie kopii zapasowych na taśmach	Łatwa konfiguracja i monitorowanie w programie DPM. Zaplanowane kopie zapasowe DPM na taśmach pozwalają na przechowywanie nawet do 99 lat. Kopie zapasowe na taśmach mogą być umieszczone poza siedzibą w celu odzyskiwania po awarii. Możesz przywrócić kopię zapasową na taśmie z dowolnego innego serwera DPM, który ma dołączoną stację/bibliotekę taśm korzystającą z tego samego typu nośnika taśm. Taśma może być szyfrowana w celu bezpiecznego magazynowania.	Opcja ta nie jest możliwa, jeśli baza danych jest przechowywana lokalnie i chcesz włączyć dodatkową ochronę. Obejściem byłoby użycie bazy danych na zdalnym serwerze SQL Server. Dziennie można zaplanować tylko jedną kopię zapasową na taśmie. Aby można było odczytać taśmę kopii zapasowej serwera DPM zawierającą kopię bazy danych, która ma zostać odzyskana, potrzebny jest działający serwer DPM z biblioteką taśm. W celu uzyskania dostępu do punktów odzyskiwania na taśmach konieczne są pewne przygotowania i specjalne kroki.
Tworzenie kopii zapasowej za pomocą natywnego wykonywania kopii zapasowych programu SQL Server na dysku lokalnym	Wbudowana w program SQL Server. Kopia zapasowa jest przechowywana na dysku lokalnym, który jest łatwo dostępny. Można ją uruchamiać zgodnie z harmonogramem, z dowolną częstotliwością. Całkowicie niezależna od programu DPM. Można zaplanować oczyszczanie pliku kopii zapasowej.	Nie jest dobrą opcją odzyskiwania po awarii, chyba że wykonane kopie zapasowe są kopiowane do lokalizacji zdalnej. Wymaga lokalnego magazynu dla kopii zapasowych, co może ograniczyć czas i częstotliwość przechowywania.

METODA TWORZENIA KOPII ZAPASOWEJ BAZY DANYCH	ZALETY	WADY
Tworzenie kopii zapasowej za pomocą natywnego wykonywania kopii zapasowych SQL i ochrony programu DPM w udziale chronionym przez program DPM	Łatwo monitorowana w programie DPM. Wiele lokalizacji plików kopii zapasowej bazy danych. Łatwo dostępna z dowolnego komputera z systemem Windows w sieci. Potencjalnie najszybsza metoda odzyskiwania.	Obsługuje tylko 64 punkty odzyskiwania. Nie jest to dobra opcja w przypadku odzyskiwania lokalizacji po awarii. Awaria serwera DPM lub dysku puli magazynów programu DPM może utrudnić odzyskiwanie. Opcja ta nie jest możliwa, jeśli baza danych programu DPM jest przechowywana lokalnie i chcesz włączyć dodatkową ochronę. Obejściem byłoby umieszczenie bazy danych DPMDB na zdalnym serwerze programu SQL Server. Aby ją skonfigurować i przetestować, konieczne są pewne dodatkowe przygotowania. W przypadku, gdy sam serwer DPM jest wyłączony, ale dyski puli magazynów DPM są w dobrym stanie, konieczny jest dodatkowy czas na przygotowania i odzyskiwanie.

METODA TWORZENIA KOPII ZAPASOWEJ BAZY DANYCH	ZALETY	WADY
Tworzenie kopii zapasowej na platformie Azure	Łatwa konfiguracja i monitorowanie w programie DPM. Wiele lokalizacji plików kopii zapasowej bazy danych. Magazyn w chmurze zapewnia niezawodne rozwiązanie odzyskiwania po awarii. Bardzo bezpieczny magazyn na bazę danych. Obsługuje 120 punktów odzyskiwania online.	Dostępna tylko w programie DPM 2012 z dodatkiem SP1 lub nowszym. Wymaga konta systemu Azure i dodatkowej konfiguracji programu DPM. Generuje pewien koszt związany z magazynem systemu Azure. Aby uzyskać dostęp do kopii zapasowych programu DPM przechowywanych w magazynie kopii zapasowych platformy Azure, - wymaga obsługiwanej wersji systemu Windows Server z usługą Azure Agent. Nie może to być inny serwer DPM. Opcja ta nie jest możliwa, jeśli baza danych jest przechowywana lokalnie i chcesz włączyć dodatkową ochronę. Obejściem byłoby użycie bazy danych na zdalnym serwerze SQL Server. Wymaga pewnego dodatkowego czasu na przygotowanie i odzyskiwanie.

METODA TWORZENIA KOPII ZAPASOWEJ BAZY DANYCH	ZALETY	WADY
Tworzenie kopii zapasowej bazy danych przez utworzenie kopii zapasowej puli magazynów programu DPM	Prosta do konfigurowania i monitorowania. Kopia zapasowa jest przechowywana na dyskach puli magazynów programu DPM i łatwo uzyskać do niej dostęp lokalnie. Zaplanowane kopie zapasowe programu DPM obsługują 512 ekspresowych pełnych kopii zapasowych. W przypadku tworzenia kopii zapasowej co godzinę masz 21 dni pełnej ochrony.	Nie jest to dobra opcja w przypadku odzyskiwania po awarii. Działa w trybie online, a odzyskiwanie może nie przebiegać zgodnie z oczekiwaniami, jeśli serwer DPM lub dysk puli magazynów ulegnie awarii. Opcja ta nie jest możliwa, jeśli baza danych jest przechowywana lokalnie i chcesz włączyć dodatkową ochronę. Obejściem byłoby użycie bazy danych na zdalnym serwerze SQL Server. Jeśli usługa DPM lub konsola nie uruchamia się lub nie działa, konieczne są pewne przygotowania i specjalne kroki w celu uzyskania dostępu do punktów odzyskiwania.
Tworzenie kopii zapasowej na pomocniczym serwerze DPM	Łatwa konfiguracja i monitorowanie w programie DPM. Zaplanowane kopie zapasowe programu DPM obsługują 512 ekspresowych pełnych kopii zapasowych. W przypadku wykonywania co godzinę umożliwią 21 dni ochrony krótkoterminowej. Jeśli będą wykonywane co 30 minut, zapewnią ochronę 10-dniową. Kopia zapasowa jest przechowywana na dyskach puli magazynów pomocniczego serwera DPM, które są dostępne lokalnie. Zapewnia dobre rozwiązanie odzyskiwania po awarii, jeśli pomocniczy serwer DPM znajduje się poza siedzibą firmy.	Wymaga dodatkowego serwera DPM i magazynu. Oba serwery DPM muszą mieć tę samą wersję programu DPM i te same pakiety zbiorcze aktualizacji.
Tworzenie kopii zapasowych na taśmach	Łatwa konfiguracja i monitorowanie w programie DPM. Zaplanowane kopie zapasowe DPM na taśmach pozwalają na przechowywanie nawet do 99 lat. Kopie zapasowe na taśmach mogą być umieszczone poza siedzibą w celu odzyskiwania po awarii. Możesz przywrócić kopię zapasową na taśmie z dowolnego innego serwera DPM, który ma dołączoną stację/bibliotekę taśm korzystającą z tego samego typu nośnika taśm. Taśma może być szyfrowana w celu bezpiecznego magazynowania.	Opcja ta nie jest możliwa, jeśli baza danych jest przechowywana lokalnie i chcesz włączyć dodatkową ochronę. Obejściem byłoby użycie bazy danych na zdalnym serwerze SQL Server. Dziennie można zaplanować tylko jedną kopię zapasową na taśmie. Aby można było odczytać taśmę kopii zapasowej serwera DPM zawierającą kopię bazy danych, która ma zostać odzyskana, potrzebny jest działający serwer DPM z biblioteką taśm. W celu uzyskania dostępu do punktów odzyskiwania na taśmach konieczne są pewne przygotowania i specjalne kroki.

METODA TWORZENIA KOPII ZAPASOWEJ BAZY DANYCH	ZALETY	WADY
Tworzenie kopii zapasowej za pomocą natywnego wykonywania kopii zapasowych programu SQL Server na dysku lokalnym	Wbudowana w program SQL Server. Kopia zapasowa jest przechowywana na dysku lokalnym, który jest łatwo dostępny. Można ją uruchamiać zgodnie z harmonogramem, z dowolną częstotliwością. Całkowicie niezależna od programu DPM. Można zaplanować oczyszczanie pliku kopii zapasowej.	Nie jest dobrą opcją odzyskiwania po awarii, chyba że wykonane kopie zapasowe są kopiowane do lokalizacji zdalnej. Wymaga lokalnego magazynu dla kopii zapasowych, co może ograniczyć czas i częstotliwość przechowywania.
Tworzenie kopii zapasowej za pomocą natywnego wykonywania kopii zapasowych SQL i ochrony programu DPM w udziale chronionym przez program DPM	Łatwo monitorowana w programie DPM. Wiele lokalizacji plików kopii zapasowej bazy danych. Łatwo dostępna z dowolnego komputera z systemem Windows w sieci. Potencjalnie najszybsza metoda odzyskiwania.	Obsługuje tylko 64 punkty odzyskiwania. Nie jest to dobra opcja w przypadku odzyskiwania lokalizacji po awarii. Awaria serwera DPM lub dysku puli magazynów programu DPM może utrudnić odzyskiwanie. Opcja ta nie jest możliwa, jeśli baza danych programu DPM jest przechowywana lokalnie i chcesz włączyć dodatkową ochronę. Obejściem byłoby umieszczenie bazy danych DPMDB na zdalnym serwerze programu SQL Server. Aby ją skonfigurować i przetestować, konieczne są pewne dodatkowe przygotowania. W przypadku, gdy sam serwer DPM jest wyłączony, ale dyski puli magazynów DPM są w dobrym stanie, konieczny jest dodatkowy czas na przygotowania i odzyskiwanie.

- W przypadku wykonywania kopii zapasowej przy użyciu grupy ochrony DPM zalecamy użycie grupy ochrony unikatowej dla bazy danych.
- Najlepszym rozwiązaniem w przypadku tworzenia kopii zapasowej na taśmie jest wykonanie co najmniej dwóch kopii taśm kopii zapasowych i przechowywanie każdej z tych kopii w innej lokalizacji zdalnej. To dodatkowa ochrona przed uszkodzeniem fizycznym i utratą taśmy kopii zapasowej.
- Jeśli wystąpienie DPM programu SQL Server nie jest uruchomione na serwerze DPM, trzeba zainstalować agenta ochrony DPM na komputerze z programem SQL Server, aby umożliwić ochronę baz danych DPM na tym serwerze.

NOTE

W przypadku przywracania instalacja programu DPM przywracanego z bazą danych DPM musi odpowiadać wersji samej bazy danych. Na przykład jeśli baza danych, którą chcesz odzyskać, pochodzi z programu DPM 2016 z instalacją Update Rollup 4, na serwerze DPM musi być uruchomiona ta sama wersja z pakietem zbiorczym aktualizacji 4. Oznacza to, że przed przywróceniem bazy danych może być konieczne odinstalowanie i ponowne zainstalowanie programu DPM w zgodnej wersji. Aby można było wyświetlić wersję bazy danych, może być konieczne ręczne zainstalowanie jej pod tymczasową nazwą, a następnie uruchomienie na tej bazie zapytania SQL sprawdzającego wersję główną i pomocniczą ostatnio zainstalowanego pakietu aktualizacji.

- Aby sprawdzić wersję bazy danych programu DPM, wykonaj następujące czynności:
 1. Aby uruchomić zapytanie, otwórz program SQL Management Studio, a następnie połącz się z wystąpieniem programu SQL, w którym działa baza danych programu DPM.
 2. Wybierz bazę danych programu DPM, a następnie uruchom nowe zapytanie.
 3. W okienku zapytania wklej i uruchom następujące zapytanie SQL:

**Select distinct MajorVersionNumber, MinorVersionNumber, BuildNumber, FileName FROM
dbo.tbl_AM_AgentPatch order by MajorVersionNumber, MinorVersionNumber,
BuildNumber**

Jeśli w wynikach zapytania nie zostanie zwrócona żadna wartość lub jeśli serwer programu DPM został uaktualniony z poprzednich wersji, ale od tamtej pory nie zainstalowano żadnego nowego zbiorczego pakietu aktualizacji, nie będzie wpisu dotyczącego głównej ani pomocniczej wersji podstawowej instalacji programu DPM. Aby sprawdzić wersje programu DPM skojarzone z pakietami zbiorczymi aktualizacji, zobacz [listy numerów kompilacji dla programu System Center Data Protection Manager \(DPM\)](#).

Tworzenie kopii zapasowej w systemie Azure

1. Przed rozpoczęciem musisz uruchomić skrypt, aby uzyskać ścieżkę punktu instalacji woluminu repliki programu DPM i wiedzieć, który punkt odzyskiwania zawiera kopię zapasową programu DPM. Zrób to po zakończeniu replikacji początkowej za pomocą usługi Kopia zapasowa Azure. W skrypcie zamień zmienną `dpmsqlservername%` na nazwę wystąpienia programu SQL Server hostującego bazę danych programu DPM.

```
Select ag.NetbiosName as ServerName,ds.DataSourceName,vol.MountPointPath
from tbl_IM_DataSource as ds
join tbl_PRM_LogicalReplica as lr on ds.DataSourceId=lr.DataSourceId
join tbl_AM_Server as ag on ds.ServerId=ag.ServerId
join tbl_SPM_Volume as vol on lr.PhysicalReplicaId=vol.VolumeSetID
and vol.Usage =1
and lr.Validity in (1,2)
where ds.datasourcename like '%dpmdb%'
and servername like '%dpmsqlservername%' --netbios name of server hosting DPMDB
```

Upewnij się, że masz kod dostępu, który został określony podczas instalacji agenta usług Azure Recovery Services i rejestracji serwera DPM w magazynie usługi Azure Backup. Ten kod dostępu jest potrzebny do przywrócenia kopii zapasowej.

2. Utwórz magazyn usługi Kopia zapasowa Azure, a następnie pobierz plik instalacyjny agenta kopii zapasowej platformy Azure i poświadczenia magazynu. Uruchom plik instalacyjny, aby zainstalować agenta na serwerze DPM i użyj poświadczeń magazynu, aby zarejestrować serwer programu DPM w magazynie. [Dowiedz się więcej](#).
3. Po skonfigurowaniu magazynu skonfiguruj grupę ochrony programu DPM zawierającą bazę danych programu DPM, a następnie wybierz opcję tworzenia jej kopii zapasowej na dysku i na platformie Azure.

Odzyskiwanie bazy danych programu DPM z platformy Azure

Bazę danych można odzyskać z platformy Azure, używając dowolnego serwera programu DPM, na którym (jest uruchomiony program DPM 2012 R2 z pakietem zbiorczym aktualizacji 7) zarejestrowany w magazynie usługi Kopia zapasowa Azure, w następujący sposób:

1. W konsoli programu DPM kliknij pozycję **Odzyskiwanie > Dodaj zewnętrzny program DPM**.
2. Podaj poświadczenia magazynu (pobierz z magazynu usługi Kopia zapasowa Azure). Weź pod uwagę, że poświadczenia są ważne tylko przez dwa dni.
3. W polu **Wybierz zewnętrzny program DPM na potrzeby odzyskiwania** wybierz serwer programu DPM, dla którego chcesz odzyskać bazę danych, wpisz hasło szyfrowania, a następnie kliknij pozycję **OK**.
4. Wybierz punkt odzyskiwania, którego chcesz używać, z listy dostępnych punktów. Kliknij pozycję **Wyczyść zewnętrzny program DPM** aby powrócić do lokalnego widoku danych programu DPM.

Tworzenie kopii zapasowej DPM database w puli magazynów programu DPM

NOTE

Ta opcja ma zastosowanie do programu DPM z Nowoczesny magazyn kopii zapasowych.

1. W konsoli programu DPM kliknij pozycję **ochrona > Utwórz grupę ochrony**.
2. Na stronie **Wybierz typ grupy ochrony** zaznacz opcję **Serwery**.
3. Na stronie **Wybierz członków grupy** wybierz pozycję **DPM Database**. Jeśli używasz SQL Server zdalnie, wybierz zainstalowaną SQL Server zdalną i wybierz pozycję DPM database. Jeśli na serwerze programu DPM jest uruchomiona SQL Server, rozwiń serwer programu DPM i wybierz pozycję DPMDB.
4. Na stronie **Wybierz metodę ochrony danych** wybierz opcję **Chcę uzyskać krótkoterminową ochronę za pomocą dysku**. Określ opcje zasady ochrony krótkoterminowej.
5. Po początkowej replikacji DPM database uruchom następujący skrypt SQL:

```
select AG.NetbiosName, DS.DatasourceName, V.AccessPath, LR.PhysicalReplicaId from tbl_IM_DataSource DS
join tbl_PRM_LogicalReplica as LR
on DS.DataSourceId = LR.DataSourceId
join tbl_AM_Server as AG
on DS.ServerId=AG.ServerId
join tbl_PRM_ReplicaVolume RV
on RV.ReplicaId = LR.PhysicalReplicaId
join tbl_STM_Volume V
on RV.StorageId = V.StorageId
where datasourcenamename like N'%dpmdb%' and ds.ProtectedGroupId is not null
and LR.Validity in (1,2)
and AG.ServerName like N'%<dpmssqlservername>%' -- <dpmssqlservername> is a placeholder, put netbios name of
server hosting DPMDB
```

Odzyskaj DPM database

Aby odtworzyć program DPM z tą samą bazą danych, należy najpierw odzyskać DPM database i zsynchronizować go z świeżo zainstalowanym programem DPM.

Wykonaj następujące kroki

1. Otwórz wiersz polecenia z uprawnieniami administracyjnymi i uruchom program *PsExec.exe -s PowerShell.exe*, aby uruchomić okno programu PowerShell w kontekście systemu.
2. Wybierz lokalizację, w której chcesz odzyskać bazę danych:

Aby skopiować bazę danych z ostatniej kopii zapasowej

1. Przejdź do ścieżki wirtualnego dysku twardego **<DPMSERVER FQDN><PhysicalReplicaId><PhysicalReplicaId>**
2. Zainstaluj plik disk0.vhdx znajdujący się w nim przy użyciu polecenia mount-VHD disk0. VHDX.
3. Po zainstalowaniu wirtualnego dysku twardego należy użyć polecenia mountvol. exe, aby przypisać literę dysku do woluminu repliki przy użyciu identyfikatora repliki fizycznej z danych wyjściowych skryptu SQL. Na przykład: mountvol X: ?\Volume{}\

Aby skopiować bazę danych z poprzedniego punktu odzyskiwania

1. Przejdź do katalogu kontenerów DPMDDB **<DPMSERVER FQDN><PhysicalReplicaId>** , zobaczysz wiele katalogów z unikatowymi identyfikatorami GUID w ramach odpowiednich punktów odzyskiwania dla bazy danych programu DPM. Katalogi inne niż przedstawiają punkt "PIT/".
2. Przejdź do dowolnej ścieżki wirtualnego dysku twardego, np. **<DPMSERVER FQDN><PhysicalReplicaId><PITId>** i Zainstaluj plik disk0.vhdx w tym pliku przy użyciu polecenia *Mount-VHD disk0.vhdx* .
3. Po zainstalowaniu wirtualnego dysku twardego należy użyć polecenia *mountvol.exe* , aby przypisać literę dysku do woluminu repliki przy użyciu identyfikatora repliki fizycznej z danych wyjściowych skryptu SQL. Na przykład: mountvol X: ?\Volume{}\

Wszystkie następujące teksty z nawiasami kątowymi w powyższych krokach są umieszczane jako posiadacze i zastępują je odpowiednimi wartościami.

- ReFSVolume — ścieżka dostępu do danych wyjściowych skryptu SQL
 - DPMServer FQDN — w pełni kwalifikowana nazwa serwera DPM
 - PhysicalReplicaId — identyfikator repliki fizycznej ze skryptu SQL out
 - PITId — identyfikator GUID inny niż identyfikator repliki fizycznej w katalogu kontenerów.
4. Otwórz inny wiersz polecenia z uprawnieniami administracyjnymi i uruchom polecenie *PsExec.exe -s cmd.exe* , aby uruchomić wiersz polecenia w kontekście systemu.
 5. Zmień katalog na dysk X: i przejdź do lokalizacji plików DPM database.
 6. Skopiuj pliki do lokalizacji, z której będzie łatwo je przywrócić. Zamknij okno CMD PsExec po skopiowaniu.
 7. Przejdź do okna programu PowerShell PsExec otwartego w kroku jeden, przejdź do ścieżki VHDX i Odinstaluj plik VHDX za pomocą polecenia *Dismount-VHD disk0.vhdx*.
 8. Po ponownym zainstalowaniu serwera programu DPM można użyć przywróconego DPMDDB do dołączenia do serwera programu DPM, uruchamiając polecenie *DPMSYNC-RESTOREDB* .
 9. Uruchom polecenie *dpmsync-Sync* po zakończeniu polecenia *dpmsync-RESTOREDB* .

Tworzenie kopii zapasowej bazy danych przez utworzenie kopii zapasowej puli magazynów programu DPM

NOTE

Ta opcja ma zastosowanie do programu DPM ze starszą wersją magazynu.

Przed rozpoczęciem musisz uruchomić skrypt, aby uzyskać ścieżkę punktu instalacji woluminu repliki programu DPM i wiedzieć, który punkt odzyskiwania zawiera kopię zapasową programu DPM. Zrób to po zakończeniu replikacji początkowej za pomocą usługi Kopia zapasowa Azure. W skrypcie zamień zmienną `dpmsqlservername%` na nazwę wystąpienia programu SQL Server hostującego bazę danych programu DPM.

```

Select ag.NetbiosName as ServerName,ds.DataSourceName,vol.MountPointPath
from tbl_IM_DataSource as ds
join tbl_PRM_LogicalReplica as lr on ds.DataSourceId=lr.DataSourceId
join tbl_AM_Server as ag on ds.ServerId=ag.ServerId
join tbl_SPM_Volume as vol on lr.PhysicalReplicaId=vol.VolumeSetID
and vol.Usage =1
and lr.Validity in (1,2)
where ds.datasourcename like '%dpmdb%'
and servername like '%dpmsqlservername%' --netbios name of server hosting DPMDB

```

1. W konsoli programu DPM kliknij pozycję **ochrona > Utwórz grupę ochrony**.
2. Na stronie **Wybierz typ grupy ochrony** zaznacz opcję **Serwery**.
3. Na stronie **Wybierz członków grupy** wybierz bazę danych programu DPM. Jeśli program SQL Server działa zdalnie, wybierz zdalnie zainstalowany program SQL Server, a następnie wybierz bazę danych programu DPM. Jeśli program SQL Server działa na serwerze programu DPM, rozwiń element serwera programu DPM i wybierz pozycję **DPMDB**.
4. Na stronie **Wybierz metodę ochrony danych** zaznacz opcję **Chcę uzyskać krótkoterminową ochronę za pomocą dysku**. Określ opcje zasad ochrony krótkoterminowej. W przypadku baz danych programu DPM zalecamy wybranie zakresu przechowywania równego dwa tygodnie.

Odzyskiwanie bazy danych

Jeśli serwer programu DPM działa nadal, a pula magazynów jest nietknięta (problemy z usługą DPM lub konsolą), skopiuj bazę danych z woluminu repliki lub kopii w tle w następujący sposób:

1. Zdecyduj, z jakiego czasu chcesz odzyskać bazę danych.
 - Jeśli chcesz skopiować bazę danych z ostatniej kopii zapasowej wykonanej bezpośrednio z woluminu repliki DPM, użyj programu **mountvol.exe**, aby przypisać literę dysku do woluminu repliki, którego identyfikator GUID znasz z danych wyjściowych skryptu SQL. Na przykład: C:\Mountvol X: \\?\Volume{d7a4fd76-a0a8-11e2-8fd3-001c23cb7375}\
 - Jeśli chcesz skopiować bazę danych z poprzedniego punktu odzyskiwania (kopii w tle), będzie konieczne utworzenie listy wszystkich kopii w tle repliki przy użyciu identyfikatora GUID woluminu z danych wyjściowych skryptu SQL. To polecenie wyświetla listę kopii w tle dla danego woluminu: C:\>Vssadmin wyświetla listę kopii w tle /dla=\\?\Volume{d7a4fd76-a0a8-11e2-8fd3-001c23cb7375}\. Zapisz czas utworzenia i identyfikator kopii w tle, z której chcesz przeprowadzić odzyskiwanie.
2. Następnie użyj programu diskshadow.exe do zamontowania kopii w tle na nieużywanej literze dysku X: za pomocą identyfikatora kopii w tle, tak aby można było skopiować pliki bazy danych.
3. Otwórz wiersz polecenia z uprawnieniami administracyjnymi i uruchom polecenie **psexec.exe -s cmd.exe**, aby uruchomić wiersz polecenia w kontekście systemowym, który pozwala uzyskać uprawnienia do nawigacji do woluminu repliki (X:), i skopiuj pliki.
4. Zmień katalog na dysk X: i przejdź do lokalizacji plików bazy danych programu DPM. Skopiuj pliki do lokalizacji, z której będzie łatwo je przywrócić. Po zakończeniu kopiowania wyjdź z okna polecenia programu psexec i uruchom program diskshadow.exe, aby ukryć wolumin X:.
5. Teraz możesz przywrócić pliki bazy danych za pomocą programu SQL Management Studio lub polecenia DPMSPYNC -RESTOREDB.

Tworzenie kopii zapasowej bazy danych na serwerze pomocniczym

1. Na pomocniczym serwerze DPM wypchnij agenta ochrony do serwera, na którym jest zainstalowana baza danych programu DPM — albo podstawowego serwera DPM, albo zdalnego serwera SQL Server. Po

zakończeniu instalacji serwer pojawi się na liście **Niechroniony serwer z agentami ochrony**, a po odświeżeniu powinien być wyświetlony stan OK.

2. Utwórz nową grupę ochrony. W obszarze **Wybierz członków grupy** wybierz serwer obsługujący bazę danych programu DPM. W obszarze **Wszystkie serwery SQL** wybierz bazę danych, która ma być chroniona. Na stronie **Wybierz metodę ochrony danych** wybierz opcję korzystania z krótkoterminowej ochrony na dysku lub w trybie online, w zależności od potrzeb. Na stronie **Określ cele krótkoterminowe** wybierz sposób skonfigurowania kopii zapasowych do krótkoterminowego przechowywania. W przypadku magazynu dyskowego możesz mieć 512 ekspresowych pełnych kopii zapasowych wykonywanych z częstotliwością nawet co 30 minut. Zakończ pracę kreatora. Ochrona zostanie uruchomiona po utworzeniu początkowego punktu odzyskiwania.

Odzyskiwanie bazy danych

1. W razie potrzeby odbuduj serwer podstawowy jako serwer DPM.
2. Aby przywrócić bazę danych, w konsoli programu DPM na serwerze pomocniczym kliknij przycisk **Odzyskiwanie** i znajdź chronioną bazę danych.
3. Wybierz datę punktu odzyskiwania, który chcesz odzyskać. Odzyskaj bazę danych do lokalizacji oryginalnej. Po odzyskiwaniu bazy danych uruchom narzędzie DPMSync.

Tworzenie kopii zapasowej bazy danych na taśmie

Musisz poznać kod kreskowy lub etykiety taśm, które zawierają kopię bazy danych programu DPM. W tym celu najlepiej zaplanować przesyłanie raportu stanu w dniu, w którym jest wykonywana kopia zapasowa bazy danych programu DPM. W raporcie zostaną uwzględnione informacje o ostatniej dacie i godzinie kopii zapasowej, etykiecie taśmy oraz kodzie kreskowym, co pozwoli zlokalizować taśmy w celu odzyskiwania. Możesz też użyć poniższego skryptu SQL do wyodrębnienia informacji z bieżącej bazy danych, aby móc zachować je oddzielnie na wypadek awarii.

```
Select Path,ro.FileSpec,media.Label,media.BarcodeValue,pd.CreationDate,
pd.ExpiryDate,pd.LifeStatus as "1=valid, 2=expired"
from dbo.tbl_MM_MediaMap mm
join dbo.tbl_MM_PhysicalDataset pd on pd.datasetid = mm.datasetid
join dbo.tbl_MM_Media media on media.MediaId = mm.MediaId
join dbo.tbl_RM_RecoverableObjectFileSpec ro on ro.DatasetId = mm.DatasetId
where ro.filespec like '%DPMDB%'
order by CreationDate desc
```

1. Utwórz grupę ochrony i na stronie **Wybierz członków grupy** wybierz program SQL Server (jeśli jest uruchomiony lokalnie, wybierz bazę danych DPMDB w obszarze serwera programu DPM).
2. Wybierz długoterminową ochronę na taśmie i określ szczegóły taśmy na stronie **Wybierz bibliotekę i szczegóły taśmy**.

Odzyskiwanie bazy danych

- Proces przywracania zależy od dostępnego sprzętu taśm i bieżącego stanu serwera DPM, na którym została wykonana kopia zapasowa na taśmie. Jeśli nie można przywrócić taśmy z serwera programu DPM, na którym wykonano kopię zapasową, trzeba przywrócić ją z innego serwera programu DPM, który ma ten sam typ stacji taśm, aby dało się odczytać taśmę. Może być konieczna odbudowa serwera DPM, jeśli jedyna dostępna stacja taśm jest dołączona do serwera DPM, który uległ awarii.
- Jeśli używasz szyfrowania taśm w programie DPM, na alternatywnym serwerze programu DPM trzeba będzie zainstalować ten sam certyfikat, który posłużył do szyfrowania taśmy.

Aby odzyskać:

1. Znajdź fizyczną taśmę zawierającą wersję, datę i godzinę bazy danych programu DPM, którą chcesz przywrócić.
2. Włóż taśmę kopii zapasowej do stacji lub biblioteki taśm i wykonaj szczegółową inwentaryzację w konsoli programu DPM -> Zarządzanie -> Biblioteki. Zauważ, że jeśli przywracasz z innego serwera programu DPM lub przywracasz do nowej instalacji programu DPM na oryginalnym serwerze, taśma będzie widoczna jako importowana (nie jako utworzona przez ten serwer programu DPM).
3. W razie potrzeby skataloguj ponownie zaimportowaną taśmę.
4. Na karcie **Odzyskiwanie** zlokalizuj źródło danych bazy danych. Jeśli pochodzi z taśmy importowanej, punkt odzyskiwania będzie wymieniony w obszarze **Zewnętrzne taśmy DPM**.
5. Odzyskaj pliki bazy danych (DPMDB). Możesz wybrać jedną z opcji: Odzyskaj do dowolnego wystąpienia programu SQL Server lub Kopiuj do folderu sieciowego. Po przywróceniu plików z taśmy kontynuuj kroki odzyskiwania przy użyciu programu SQL Management Studio lub polecenia DPMSYNC -RESTOREDB.

Tworzenie kopii zapasowej za pomocą natywnego wykonywania kopii zapasowych programu SQL Server na dysku lokalnym

Możesz po prostu utworzyć kopię bazy danych programu DPM na dysku lokalnym za pomocą natywnego wykonywania kopii zapasowych programu SQL Server, niezależnie od programu DPM.

1. Zapoznaj się z [opisem](#) kopii zapasowych programu SQL Server.
2. [Dowiedz się więcej](#) o tworzeniu kopii zapasowych programu SQL Server w chmurze.

Tworzenie kopii zapasowej za pomocą natywnego wykonywania kopii zapasowych programu SQL Server w udziale chronionym przez program DPM

Ta opcja kopii zapasowej wykorzystuje natywną funkcjonalność SQL w celu wykonania kopii zapasowej bazy danych programu DPM w udziale, chroni udział za pomocą programu DPM i korzysta z wcześniejszych wersji usługi VSS systemu Windows w celu przywracania.

Przed rozpoczęciem

1. Jeśli baza danych programu DPM znajduje się na zdalnym serwerze SQL Server, zainstaluj na tym serwerze agenta programu DPM.
2. W programie SQL Server utwórz folder na dysku z wystarczającą ilością wolnego miejsca do zapisania pojedynczej kopii kopii zapasowej. Na przykład: C:\DPMBACKUP.
3. Udostępnij ten folder. Na przykład udostępnij folder C:\DPMBACKUP jako DPMBACKUP.
4. Skopiuj i wklej poniższe polecenie OSQL do Notatnika i zapisz je w pliku o nazwie C:\DPMBACKUP\bkupdb.cmd. Upewnij się, że plik nie ma rozszerzenia .txt. Zmień SQL_Instance_name i DPMDB_NAME, aby odpowiadały nazwom wystąpienia i bazy danych DPMDB używanym przez serwer programu DPM.

```
OSQL -E -S localhost\SQL_INSTANCE_NAME -Q "BACKUP DATABASE DPMDB_NAME TO DISK='C:\DPMBACKUP\dpmdb.bak' WITH FORMAT"
```

5. Za pomocą Notatnika otwórz plik ScriptingConfig.xml znajdujący się w folderze ...\\DPM\\Scripting.

- Na zdalnym serwerze SQL Server: **C:\Program Files\Microsoft Data Protection**

Manager\DPM\Scripting

- Na serwerze DPM: **C:\Program Files\Microsoft System Center\DPM\DPM\Scripting**

6. Zmodyfikuj plik ScriptingConfig.xml i zmień DataSourceName= na literę dysku, który zawiera folder/udział DPMDDBBACKUP. Zmień wpis PreBackupScript na pełną ścieżkę i nazwę pliku bkupdb.cmd zapisanego w kroku 5.

```
<?xml version="1.0" encoding="utf-8"?>
<ScriptConfiguration xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns="https://schemas.microsoft.com/2003/dls/ScriptingConfig.xsd">
  <DataSourceScriptConfig DataSourceName="C:">
    <PreBackupScript>C:\DPMDDBBACKUP\bkupdb.cmd</PreBackupScript>
    <Timeout>120</Timeout>
  </DataSourceScriptConfig>
</ScriptConfiguration>
```

7. Zapisz zmiany w pliku ScriptingConfig.xml.
8. Chroń folder C:\DPMBACKUP lub udział \\sqlservername\DPMBACKUP za pomocą programu DPM i poczekaj na utworzenie repliki początkowej. W folderze C:\DPMBACKUP powinien pojawić się plik dpmdb.bak jako wynik uruchomienia skryptu przed utworzeniem kopii zapasowej, który z kolei został skopiowany do repliki DPM.
9. Jeśli odzyskiwanie samoobsługowe nie zostało włączone, będą potrzebne dodatkowe kroki w celu udostępnienia folderu DPMBACKUP w replicie:
 - a. W konsoli programu DPM > **Ochrona** Znajdź źródło danych DPMBACKUP i zaznacz je. W sekcji szczegółów kliknij przycisk **Kliknij, aby wyświetlić szczegóły** obok linku do ścieżki repliki i skopiuj ścieżkę do Notatnika. Usuń ścieżkę źródłową i zachowaj ścieżkę docelową. Ścieżka powinna wyglądać podobnie do następującej: **C:\Program Files\Microsoft System Center\DPM\DPM\Volumes\Replica\File System \ vol_c9aea05f-31e6-45e5-880c-92ce5fba0a58 \ 454d81a0-0d9d-4e07-9617-d49e3f2aa5de \ Full \ DPMBACKUP**.
 - b. Utwórz udział do tej ścieżki o nazwie **DPMSEVERNAME-DPMDB**. Możesz użyć poniższego polecenia Net Share w wierszu polecenia z uprawnieniami administracyjnymi.

```
Net Share DPMSEVERNAME-dpmdb="C:\Program Files\Microsoft System
Center\DPM\DPM\Volumes\Replica\File System\vol_c9aea05f-31e6-45e5-880c-92ce5fba0a58\454d81a0-
0d9d-4e07-9617-d49e3f2aa5de\Full\DPMBACKUP"
```

Konfigurowanie kopii zapasowej

Możesz utworzyć kopię zapasową bazy danych programu DPM w taki sposób, jak każdej innej bazy danych programu SQL Server, przy użyciu natywnych operacji kopii zapasowych programu SQL Server.

- Zapoznaj się z [opisem](#) kopii zapasowych programu SQL Server.
- [Dowiedz się więcej](#) o tworzeniu kopii zapasowych programu SQL Server w chmurze.

Odzyskiwanie bazy danych

1. Nawiąż połączenie z udziałem \\DPMSEVERNAME\DPMSERVERNAME-dpmdb za pomocą Eksploratora z dowolnego komputera z systemem Windows.
2. Kliknij prawym przyciskiem myszy plik dpmdb.bak, aby wyświetlić właściwości. Na karcie **Poprzednie wersje** znajdują się wszystkie kopie zapasowe, które można wybrać i skopiować. Ponadto najnowsza kopia zapasowa nadal znajduje się w folderze C:\DPMBACKUP, który również jest łatwo dostępny.

3. Jeśli potrzebujesz przenieść dysk puli magazynów DPM dołączony do sieci SAN do innego serwera, aby był możliwy odczyt z woluminu repliki, lub ponownie zainstalować system Windows w celu odczytu dysków przyłączonych lokalnie, musisz wcześniej znać ścieżkę punktu instalacji woluminu repliki DPM lub identyfikator GUID woluminu, aby wiedzieć, który wolumin przechowuje kopię zapasową bazy danych. Aby wyodrębnić te informacje w dowolnej chwili po rozpoczęciu ochrony, ale zanim zajdzie potrzeba przywrócenia, możesz użyć poniższego skryptu SQL. Zastąp zmienną %dpmsqlservername% nazwą serwera SQL Server zawierającego bazę danych.

```
Select ag.NetbiosName as
ServerName,ds.DataSourceName,vol.MountPointPath,vol.GuidName
from tbl_IM_DataSource as ds
join tbl_PRM_LogicalReplica as lr on ds.DataSourceId=lr.DataSourceId
join tbl_AM_Server as ag on ds.ServerId=ag.ServerId
join tbl_SPM_Volume as vol on lr.PhysicalReplicaId=vol.VolumeSetID
and vol.Usage =1
and lr.Validity in (1,2)
where ds.datasourcenamename like '%C:\%' -- volume drive letter for DPMBACKUP
and servername like '%dpmsqlservername%' --netbios name of server hosting DPMDB
```

4. Jeśli chcesz odzyskać dane po przeniesieniu dysków puli magazynów programu DPM lub po odbudowie serwera DPM:

- a. Wolumin ma identyfikator GUID. W razie potrzeby zamontowania woluminu na innym serwerze Windows lub po odbudowie serwera DPM użyj programu mountvol.exe, aby przypisać literę dysku, korzystając z identyfikatora GUID woluminu pobranego z danych wyjściowych skryptu SQL:

C:\Mountvol X: \\?\Volume{d7a4fd76-a0a8-11e2-8fd3-001c23cb7375}\ .

- b. Udostępnij ponownie folder DPMBACKUP na woluminie repliki za pomocą litery dysku i części ścieżki repliki reprezentującej strukturę folderów.

```
net share SERVERNAME-DPMB="X:\454d81a0-0d9d-4e07-9617-d49e3f2aa5de\Full\DPMBACKUP"
```

- c. Nawiąż połączenie z udziałem \\SERVERNAME\DPMSERVERNAME-dpmbd za pomocą Eksploratora z dowolnego komputera z systemem Windows
- d. Kliknij prawym przyciskiem myszy plik dpmbd.bak, aby wyświetlić właściwości. Na karcie **Poprzednie wersje** znajdują się wszystkie kopie zapasowe, które można wybrać i skopiować.

Zarządzanie odzyskiwaniem po awarii programu DPM: kopia zapasowa bazy danych programu DPM

Jednym ze sposobów odbudowy serwera programu DPM w tej samej bazie danych jest utworzenie kopii zapasowej bazy danych programu DPM na dyskach lokalnych.

DPM database zawiera konfigurację programu DPM wraz z danymi dotyczącymi kopii zapasowych programu DPM. W przypadku awarii można ponownie skompilować funkcjonalność serwera programu DPM, używając najnowszej kopii zapasowej bazy danych na dysku lokalnym. Jeśli serwer DPM ulegnie awarii lub stanie się niedziałający, a nadal masz niezmienną pulę magazynów zawierającą kopie zapasowe, możesz ponownie skonfigurować serwer programu DPM za pomocą tej samej bazy danych programu DPM.

Upewnij się że

1. Kopia zapasowa bazy danych programu DPM na dyskach lokalnych
2. Pula magazynów powinna być nienaruszona i dostępna.

Tworzenie kopii zapasowej DPM database

1. W konsoli programu DPM kliknij pozycję **ochrona** > **Utwórz grupę ochrony**.
2. Na stronie **Wybierz typ grupy ochrony** zaznacz opcję **Serwery**.
3. Na stronie **Wybierz członków grupy** wybierz pozycję **DPM Database**. Jeśli używasz SQL Server zdalnie, wybierz zainstalowaną SQL Server zdalną i wybierz pozycję DPM database. Jeśli na serwerze programu DPM jest uruchomiona SQL Server, rozwiń serwer programu DPM i wybierz pozycję DPMDB.
4. Na stronie **Wybierz metodę ochrony danych** wybierz opcję **Chcę uzyskać krótkoterminową ochronę za pomocą dysku**. Określ opcje zasady ochrony krótkoterminowej.
5. Po początkowej replikacji DPM database. Uruchom następujący skrypt SQL:

```
select AG.NetbiosName, DS.DatasourceName, V.AccessPath, LR.PhysicalReplicaId from tbl_IM_DataSource DS
join tbl_PRM_LogicalReplica as LR
on DS.DataSourceId = LR.DataSourceId
join tbl_AM_Server as AG
on DS.ServerId=AG.ServerId
join tbl_PRM_ReplicaVolume RV
on RV.ReplicaId = LR.PhysicalReplicaId
join tbl_STM_Volume V
on RV.StorageId = V.StorageId
where datasourcenamename like N'%dpmdb%' and ds.ProtectedGroupId is not null
and LR.Validity in (1,2)
and AG.ServerName like N'%<dpmsqlservername>%' -- <dpmsqlservername> is a placeholder, put netbios name
of server hosting DPMDB
```

Odzyskaj DPM database

Aby odtworzyć program DPM z tą samą bazą danych, należy najpierw odzyskać DPM database i zsynchronizować go z świeżo zainstalowanym programem DPM.

Wykonaj następujące czynności:

1. Otwórz wiersz polecenia z uprawnieniami administracyjnymi i uruchom program PsExec. exe-s PowerShell. exe, aby uruchomić okno programu PowerShell w kontekście systemu.
2. Zdecyduj, z której chcesz odzyskać bazę danych:

Aby skopiować bazę danych z ostatniej kopii zapasowej

1. Przejdź do ścieżki wirtualnego dysku twardego, np. <DPMServer FQDN ><PhysicalReplicaId >
<PhysicalReplicaId >
2. Zainstaluj plik disk0. vhdx znajdujący się w nim przy użyciu pliku Mount-VHD disk0. vhdx
3. Po zainstalowaniu wirtualnego dysku twardego należy użyć polecenia mountvol. exe, aby przypisać literę dysku do woluminu repliki przy użyciu identyfikatora repliki fizycznej z danych wyjściowych skryptu SQL. Na przykład: mountvol X: \? \Volume{<PhysicalReplicaId>} \

Aby skopiować bazę danych z poprzedniego punktu odzyskiwania

1. Przejdź do katalogu kontenerów DPMDB, czyli <ReFSVolume><DPMServer FQDN ><PhysicalReplicaId >, zostanie wyświetlonych wiele katalogów z unikatowymi identyfikatorami GUID w ramach odpowiednich punktów odzyskiwania dla bazy danych programu DPM. Katalogi inne niż przedstawiają punkt "PIT/"
2. Przejdź do dowolnej ścieżki wirtualnego dysku twardego, np. <ReFSVolume><DPMServer FQDN >
<PhysicalReplicaId ><PITId > i Zainstaluj plik disk0. vhdx w tym pliku przy użyciu pliku Mount-VHD disk0. VHDX.
3. Po zainstalowaniu wirtualnego dysku twardego należy użyć polecenia mountvol. exe, aby przypisać literę

dysku do woluminu repliki przy użyciu identyfikatora repliki fizycznej z danych wyjściowych skryptu SQL.
Na przykład: mountvol X: \? \Volume{<PhysicalReplicaId>} \

Wszystkie następujące teksty z nawiasami kątowymi w powyższych krokach są umieszczane jako posiadacze i zastępują je odpowiednimi wartościami.

- ReFSVolume — ścieżka dostępu do danych wyjściowych skryptu SQL
 - DPMServer FQDN — w pełni kwalifikowana nazwa serwera DPM
 - PhysicalReplicaId — identyfikator repliki fizycznej ze skryptu SQL out
 - PITId — identyfikator GUID inny niż identyfikator repliki fizycznej w katalogu kontenerów.
4. Otwórz inny wiersz polecenia z uprawnieniami administracyjnymi i uruchom polecenie PsExec. exe-s cmd. exe, aby uruchomić wiersz polecenia w kontekście systemu.
 5. Zmień katalog na dysk X: i przejdź do lokalizacji plików DPM database.
 6. Skopiuj pliki do lokalizacji, z której będzie łatwo je przywrócić. Zamknij okno CMD PsExec po skopiowaniu.
 7. Przejdź do okna programu PowerShell PsExec otwartego w kroku jeden, przejdź do ścieżki VHDX i Odinstaluj plik VHDX za pomocą polecenia Dismount-VHD disk0. VHDX.
 8. Po ponownym zainstalowaniu serwera programu DPM można użyć przywróconego DPMDB do dołączenia do serwera programu DPM, uruchamiając polecenie DPMSYNC-RESTOREDB.
 9. Uruchom polecenie DPMSYNC-SYNC po zakończeniu polecenia DPMSYNC-RESTOREDB.

Monitorowanie programu DPM

07.03.2020 • 15 minutes to read

Można monitorować pojedynczy serwer programu System Center Data Protection Manager (DPM) z konsoli administratora programu DPM, wielu serwerów programu DPM z poziomu konsoli centralnej lub monitorować działanie programu DPM z Operations Manager.

Monitorowanie za pomocą konsoli programu DPM

Aby monitorować program DPM w konsoli programu, należy zalogować się na serwerze programu DPM przy użyciu konta administratora lokalnego. Oto co można monitorować:

- Na karcie **Alerty** można monitorować błędy, ostrzeżenia i informacje ogólne dotyczące grupy ochrony lub określonego chronionego komputera. Można też przeglądać komunikaty według ich ważności. Można wyświetlać aktywne i nieaktywne alerty oraz konfigurować powiadomienia e-mail.
- Na karcie **Zadania** można zobaczyć zadania inicjowane przez program DPM dla określonego chronionego komputera lub grupy ochrony. Można też śledzić postępy zadań lub sprawdzać zasoby używane przez te zadania.
- W obszarze zadania **Ochrona** można sprawdzić stan woluminów i udziałów w grupie ochrony oraz sprawdzić ustawienia konfiguracji, takie jak ustawienia odzyskiwania, przydział dysku i harmonogram tworzenia kopii zapasowych.
- W obszarze zadania **Zarządzanie** na karcie **Dyski**, **Agenci** i **Biblioteki** można sprawdzić stan taśm i bibliotek taśm, dysków w puli magazynów oraz stan wdrożonego agenta programu DPM.

Monitorowanie programu DPM za pomocą konsoli centralnej

Program Central Console to konsola programu System Center Operations Manager, którą można wdrożyć w celu monitorowania wielu serwerów programu DPM i zarządzania nimi w jednym miejscu. W konsoli centralnej można monitorować i śledzić stan wielu serwerów programu DPM oraz zadań, taśm, magazynu, grup ochrony i miejsca na dysku.

- W **widoku zadań** można wyświetlić listę zadań uruchomionych na wszystkich serwerach programu DPM monitorowanych przez konsolę centralną.
- W **widoku alertów** można uzyskać listę wszystkich alertów programu DPM, które wymagają akcji. Opcja **Rozwiązywanie problemów** pozwala uzyskać więcej szczegółów dotyczących danego alertu.

Alerty wyświetlane w konsoli można łączyć. Powtarzające się alerty można wyświetlić jako jeden alert, tak samo jak w przypadku alertów, które mają taką samą główną przyczynę. Jeśli używasz systemu biletów, możesz wygenerować jeden bilet tylko dla powtórzonych alertów.

- W **widoku stanu** można uzyskać informacje o stanie obiektów programu DPM.

Monitorowanie programu DPM za pomocą konsoli platformy Azure

Pulpit nawigacyjny umożliwia szybkie przeglądanie stanu kopii zapasowych programu System Center — Data Protection Manager (DPM) w systemie Windows Azure Backup. Pulpit nawigacyjny to centralna brama umożliwiająca podgląd serwerów chronionych przez magazyny kopii zapasowych:

- Obszar **Przegląd użycia** zawiera informacje na temat korzystania z magazynu kopii zapasowych. Można

wybrać magazyn, aby wyświetlić informacje o miejscu używanym przez magazyn oraz o miejscu udostępnionym w ramach subskrypcji. Jest również widoczna liczba serwerów zarejestrowanych w magazynie.

- Obszar **Szybki dostęp** zawiera najważniejsze informacje o konfiguracji magazynu kopii zapasowych. Informuje, czy magazyn jest online, jaki jest do niego przypisany certyfikat, kiedy wygasa certyfikat, jaka jest geograficzna lokalizacja serwerów magazynu oraz jakie są szczegóły subskrypcji usługi.

Z poziomu pulpitu nawigacyjnego można pobrać agenta kopii zapasowej do zainstalowania na serwerze, zmodyfikować ustawienia certyfikatów przekazanych do magazynu i w razie potrzeby usunąć magazyn.

Centralne monitorowanie

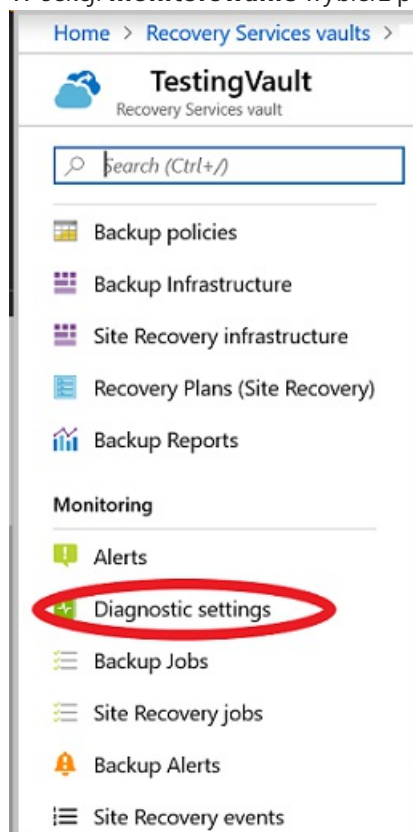
Wszyscy klienci programu DPM (połączeni z platformą Azure) mogą korzystać z funkcji monitorowania centralnego, rozwiązania monitorującego dostępnego w Microsoft Azure Backup. Można monitorować zarówno kopie zapasowe lokalne, jak i w chmurze, korzystając z Log Analytics z centralnym monitorowaniem. To rozwiązanie do monitorowania służy do monitorowania parametrów tworzenia kopii zapasowych kluczy, takich jak zadania tworzenia kopii zapasowych, alerty dotyczące tworzenia i magazynowania w chmurze, w ramach wszystkich magazynów usługi Recovery & subskrypcje. Możesz również tworzyć powiadomienia o alertach i otwierać bilety przy użyciu elementów webhook lub integracji narzędzia ITSM.

NOTE

Aby móc centralnie monitorować, musisz mieć ważną subskrypcję platformy Azure.

Włącz monitorowanie centralne

1. Zaloguj się do Azure Portal.
2. [Utwórz magazyn usługi Recovery Service](#) lub, jeśli już istnieje, wybierz tę samą opcję.
3. W sekcji **monitorowanie** wybierz pozycję **Ustawienia diagnostyczne**.



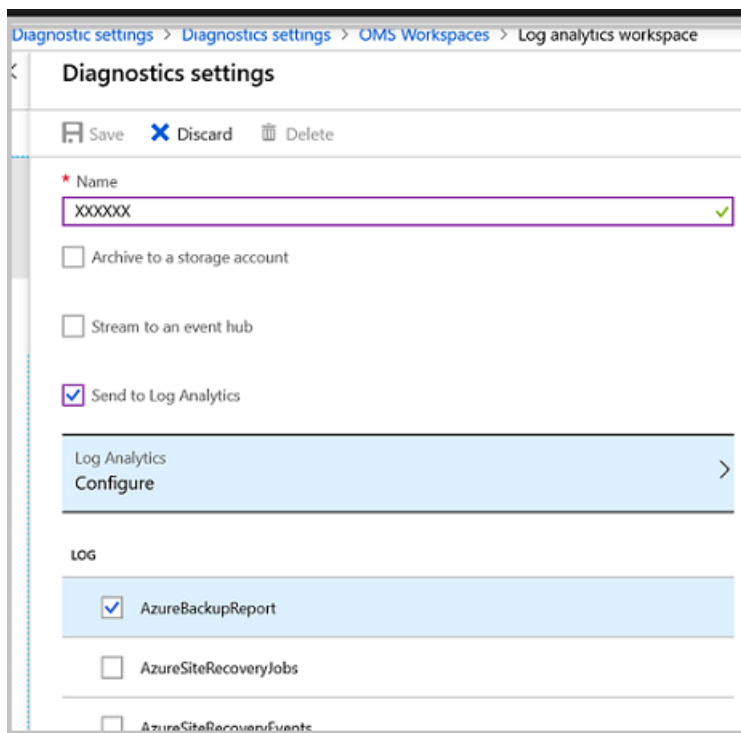
4. Kliknij pozycję **Włącz ustawienia diagnostyczne**.

5. W oknie **Ustawienia diagnostyczne** podaj prawidłową nazwę ustawienia, wybierz pozycję **Wyślij do log Analytics**, wybierz odpowiedni obszar roboczy usługi log Analytics lub [Utwórz go](#), wybierz odpowiedni dziennik, *AzureBackupReport* i kliknij przycisk **Zapisz**.

NOTE

Wybierz ten sam obszar roboczy dla wszystkich magazynów, aby uzyskać scentralizowany widok w obszarze roboczym. Poczekać 24 godziny na zakończenie wypychania danych po zakończeniu konfiguracji.

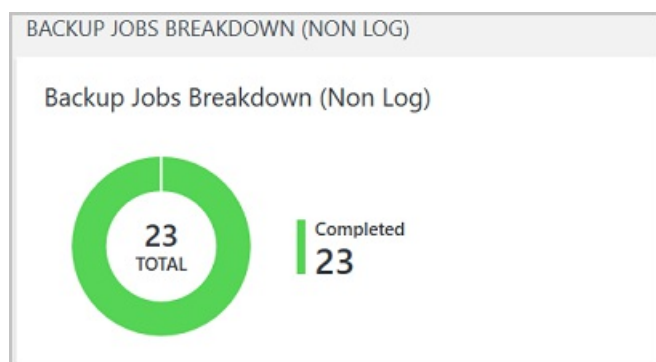
Oto przykładowy raport dotyczący kopii zapasowej:



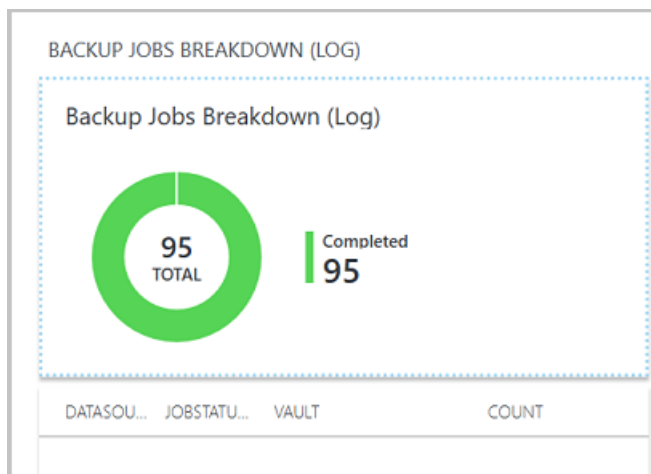
Monitorowanie danych kopii zapasowej

1. Wybierz obszar roboczy Log Analytics.
2. Kliknij pozycję **Portal pakietu OMS**. Zostanie wyświetlony pulpit nawigacyjny rozwiązania zawierający wszystkie informacje o kopii zapasowej, jak pokazano poniżej:

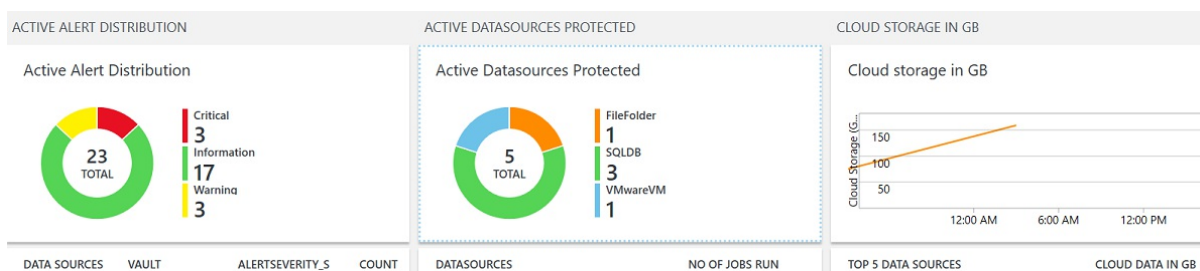
Przykład 1:



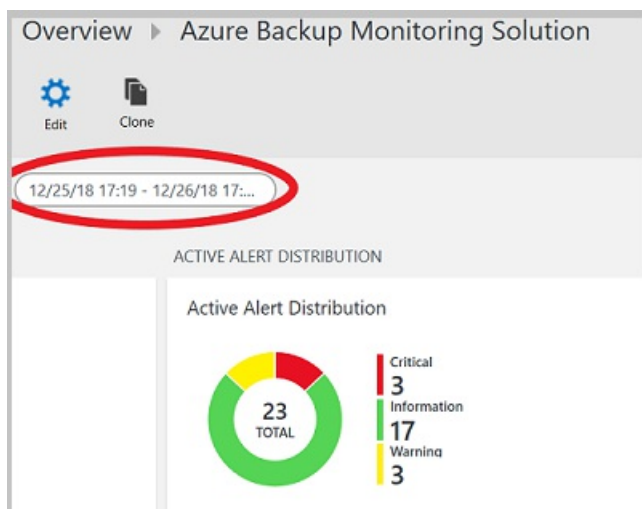
Przykład 2:



3. Można również monitorować aktywne alerty, bieżące źródła danych, których kopie zapasowe są tworzone, oraz magazynu w chmurze, jak pokazano poniżej:



4. Możesz również określić żądany zakres czasu dla monitorowania parametrów kopii zapasowej.



Tworzenie alertów niestandardowych

1. Kliknij dowolne wartości na powyższym wykresie, aby wyświetlić więcej szczegółów w oknie dzienniki.
2. Kliknij ikonę **alertu**.
3. Wybierz pozycję **Przejdź do alertów platformy Azure**.
4. W obszarze roboczym Log Analytics kliknij pozycję **Nowa reguła alertu**.
5. Zdefiniuj **warunek alertu**, **szczegóły alertu** i **grupę akcji**.
6. [Dowiedz się więcej](#) o konfigurowaniu nowych alertów.

Monitorowanie programu DPM przy użyciu programu Operations Manager

Można monitorować i raportować kondycję i stan serwerów programu DPM przy użyciu pakietów administracyjnych programu System Center Operations Manager dla programu DPM. Program DPM udostępnia

następujące pakiety administracyjne, które są stosowane w odniesieniu do używanej wersji programu DPM:

- **Pakiet administracyjny raportowania** (Microsoft.SystemCenter.DataProtectionManager.Reporting.MP)
— zbiera i wyświetla dane raportowania z wszystkich serwerów programu DPM i ujawnia zestaw Operations Manager widoków magazynu dla programu DPM. Można tworzyć zapytania dotyczące tych widoków, aby generować raporty niestandardowe.
- **Pakiet administracyjny odnajdywania i monitorowania**
(Microsoft.SystemCenter.DataProtectionManager.Discovery.MP)
- **Pakiet administracyjny biblioteki** — (Microsoft.Center.dataprotectionmanager.Library)

Za pomocą tych pakietów można:

- Centralnie monitorować kondycję i stan serwerów programu DPM, chronionych serwerów i komputerów oraz kopii zapasowych.
- Wyświetlać stan wszystkich ról na serwerach programu DPM oraz chronionych źródeł danych. Monitorować, identyfikować, podejmować działania i rozwiązywać problemy dotyczące alertów.
- Używać alertów programu Operations Manager do monitorowania pamięci serwera programu DPM, procesora, zasobów dysku i bazy danych.
- Monitorować trendy wydajności i użycia zasobów na serwerach programu DPM.

Wymagania wstępne

- Do korzystania z pakietów administracyjnych programu DPM wymagany jest serwer System Center Operations Manager uruchomiony. Magazyn danych programu Operations Manager musi być uruchomiony i działać prawidłowo.
- Jeśli używasz wcześniejszej wersji pakietów administracyjnych odnajdywania i biblioteki uzyskanych z nośnika instalacyjnego programu DPM, należy usunąć je z serwera programu DPM i zainstalować nowe wersje ze strony pobierania.
- Można uruchamiać tylko jedną wersję językową pakietu administracyjnego naraz. Aby użyć pakietu w innym języku, należy odinstalować pakiet w istniejącym języku, a następnie zainstalować go w nowym języku.
- Jeśli na serwerze programu Operations Manager są zainstalowane wcześniejsze wersje pakietu administracyjnego programu DPM, należy je usunąć przed zainstalowaniem nowego pakietu.

Konfigurowanie pakietów administracyjnych

Zainstaluj agenta programu Operations Manager na każdym serwerze programu DPM, który chcesz monitorować. Następnie uzyskaj pakiety administracyjne, zaimportuj pakiety administracyjne odnajdywania i biblioteki, zainstaluj konsolę centralną programu DPM i zaimportuj pakiet administracyjny raportowania.

Instalowanie agenta i uzyskiwanie pakietów administracyjnych

1. Informacje na temat opcji instalacji agenta zawiera artykuł [Metody instalacji programu Operations Manager](#). Aby uzyskać najnowszą wersję agenta, odwiedź stronę [Microsoft Monitoring Agent](#) w Centrum pobierania.
2. Pobierz pakiety z [Centrum pobierania](#). Pobrane pakiety administracyjne odnajdywania i biblioteki są umieszczane w folderze C:\Program Files\System Center Management Packs. Pakiet administracyjny raportowania jest umieszczany w oddzielnym folderze wewnątrz tego folderu.

Importowanie pakietów administracyjnych

Importowanie pakietów administracyjnych odnajdywania i biblioteki Zaloguj się na serwerze programu Operations Manager za pomocą konta, które jest elementem członkowskim roli Administratorzy programu Operations Manager. Pamiętaj, aby usunąć wszystkie poprzednie wersje pakietów administracyjnych biblioteki lub odnajdywania działające na serwerze.

1. W konsoli Operacje kliknij pozycję **Administracja**. Kliknij prawym przyciskiem myszy pozycję **Pakiety administracyjne** > **Importuj pakiety administracyjne**. Wybierz pozycję **Microsoft.SystemCenter.DataProtectionManagerDiscovery.MP** > **Otwórz**, a następnie pozycję **Microsoft.SystemCenter.DataProtectionManagerLibrary.MP** > **Otwórz**
2. Postępuj zgodnie z instrukcjami kreatora Importowanie pakietów administracyjnych. Więcej informacji dotyczących uruchamiania tego kreatora zawiera artykuł [How to Import an Operations Manager Management Pack](#) (Jak zaimportować pakiet administracyjny programu Operations Manager).

Konfigurowanie programu Central Console

Musisz zainstalować konsolę centralną programu DPM na serwerze programu Operations Manager. Ta konsola służy do zarządzania wieloma serwerami programu DPM w programie Operations Manager.

1. W programie Operations Manager na ekranie **Konfiguracja** wykonaj następujące czynności:
 - Wybierz opcję **Zainstaluj serwer konsoli centralnej i składniki po stronie klienta**, jeśli chcesz monitorować serwery programu DPM przy użyciu pakietu administracyjnego oraz zarządzać ustawieniami i konfiguracją serwerów programu DPM za pomocą konsoli centralnej.
 - Wybierz opcję **Zainstaluj składniki serwera konsoli centralnej po stronie serwera**, jeśli chcesz monitorować serwery programu DPM przy użyciu pakietu administracyjnego, ale nie chcesz zarządzać ustawieniami i konfiguracją serwerów programu DPM za pomocą konsoli centralnej.
2. Program DPM dodaje wyjątki zapory dla portu 6075 konsoli. Należy także otworzyć porty dla plików SQL Server.exe i SQL browser.exe

Importowanie pakietu administracyjnego raportowania

1. Zaloguj się do serwera programu Operations Manager za pomocą konta, które jest elementem członkowskim roli Administratorzy programu Operations Manager.
2. W konsoli Operacje kliknij pozycję **Administracja**. Kliknij prawym przyciskiem myszy pozycję **Pakiety administracyjne** > **Importuj pakiety administracyjne**.
3. Wybierz pozycję **Microsoft.SystemCenter.DataProtectionManagerReporting.MP** > **Otwórz**. Postępuj zgodnie z instrukcjami kreatora Importowanie pakietów administracyjnych.

Dostosowywanie ustawień pakietu administracyjnego

Po zaimportowaniu pakietu administracyjnego znajdują i monitorują dane bez konieczności dodatkowej konfiguracji. Można opcjonalnie dostosować ustawienia, takie jak monitory i reguły dla danego środowiska. Na przykład jeśli okaże się, że włączone zasady pomiaru wydajności obniżają wydajność serwerów mających wolne łącza sieci WAN, można je wyłączyć. Odpowiednie instrukcje można znaleźć w artykule [How to enable or disable a rule or monitor](#) (Jak włączyć lub wyłączyć regułę lub monitor).

Konfigurowanie rejestrowania w programie DPM

11.12.2019 • 7 minutes to read

Działanie rejestruje działania programu System Center Data Protection Manager (DPM) w plikach dziennika (*.errlog). Pliki dziennika są rozdzielane tabulatorami i można je otwierać w programie Excel w celu łatwego wyświetlania. Można filtrować przy użyciu określonych poziomów oraz identyfikatorów zadań w celu znalezienia interesujących zdarzeń. Każdy wpis dziennika ma identyfikator zadania dziennika wygenerowany w programie DPM jako unikatowy identyfikator GUID dla każdego zadania programu DPM. Ułatwia to śledzenie wpisów dziennika dla poszczególnych zadań. Pliki dziennika znajdują się w następujących lokalizacjach:

- **Informacje o instalacji programu DPM:** zarejestrowane na serwerze DPM w systemie%ProgramFiles%\Microsoft System Center\DPM\DPMLogs.
- **Informacje o działaniu programu DPM:** zarejestrowane na serwerze DPM w systemie%ProgramFiles%\Microsoft System Center\DPM\DPM\Temp.
- **Działanie chronionego klienta:** rejestrowane na komputerze klienckim w folderze %ProgramFiles%\Microsoft Data Protection Manager\DPM\Temp Logs. Działania inicjowane przez klienta, takie jak samoobsługowe odzyskiwanie, są rejestrowane na komputerze klienckim w oparciu o użytkownika (%USERPROFILE%\AppData\Roaming\Microsoft\System Center Data Protection Manager\).

Ustawienia pliku dziennika można dostosować w następujący sposób:

NAZWA WARTOŚCI	TYP WARTOŚCI/DOZWOLONE WARTOŚCI	SZCZEGÓŁY
----------------	---------------------------------	-----------

NAZWA WARTOŚCI	TYP WARTOŚCI/DOZWOLONE WARTOŚCI	SZCZEGÓŁY
TraceLogLevel	DWORD TRACE_ERROR — rejestruje wszystkie błędy i niepowodzenia — ustawienie domyślne TRACE_DBG_ACTIVITY — rejestruje wszystkie działania, takie jak uruchamianie, anulowanie i kończenie TRACE_DBG_NORMAL — rejestruje działania uznawane za ważne TRACE_DBG_CRITICAL — rejestruje tylko błędy krytyczne. TRACE_DBG_FATAL — rejestruje błędy krytyczne, takie jak niepowodzenia zadań	Określa poziom rejestrowania. Może być przesłonięta na poziomie pliku binarnego. Prawidłowa maska bitów dozwolonych wartości to: <pre>enum TRACE_FLAG{ TRACE_ERROR = 0x2, TRACE_DBG_ACTIVITY = 0x4, TRACE_DBG_ = 0x8, TRACE_PERF = 0x20, TRACE_DBG_FATAL = 0x200, TRACE_DBG_CRITICAL = 0x400 };</pre> Można również włączyć rejestrację pełną, ale należy pamiętać, że ma to wpływ na wydajność. Jeśli to konieczne w ograniczonym okresie, wykonaj następujące czynności: 1. w rejestrze w HKLM\Software\Microsoft\Microsoft Data Protection Manager dodać wartość DWORD TraceLogLevel i ustawić ją na pozycji 0x43e. 2. Aby zastosować natychmiast, Zatrzymaj usługi DPM, dla których chcesz włączyć pełne rejestrowanie, i usuń stare dzienniki. 3. po odtworzeniu problemu i zakończeniu rozwiązywania problemów Usuń utworzony wpis rejestru i uruchom ponownie zatrzymane usługi, aby Rejestracja niepełna będzie działać ponownie.
TraceLogPath	REG_SZ	Określa lokalizację dziennika. Wymaga prawidłowej ścieżki woluminu NTFS z 3 GB skompresowanego miejsca na serwerze DPM (nazwy ścieżek zawierających spacje nie wymagają cudzysłowu). Może być przesłonięta na poziomie pliku binarnego.

NAZWA WARTOŚCI	TYP WARTOŚCI/DOZWOLONE WARTOŚCI	SZCZEGÓŁY
TraceLogMaxSize	DWORD	Określa rozmiar pliku dziennika Domyślnie 5 MB Rozmiar pliku (całkowite miejsce na dysku zużyte dla dziennika binarnego = rozmiar * liczba plików do zachowania)
TraceLogMaxNum	DWORD	Maksymalna liczba plików dziennika do zachowania Domyślnie 30 Bieżąca liczba plików dziennika jest śledzona w HKLM\Software\Microsoft\Microsoft Data Protection Manager: <Binary>TraceLogNextNum (DWORD). Jest to wewnętrzny klucz rejestru. Nie zaleca się jego modyfikacji.

Mapowanie plików binarnych i usług

Mapowania pomiędzy niektórymi nazwami plików binarnych dziennika a usługami przedstawiono w poniższej tabeli.

USŁUGA/PROCES	NAZWA PLIKU BINARNEGO	SZCZEGÓŁY
Aparat programu DPM (MSDPM)	MSDPM	Dzienniki aparatu MSDPM zawierają informacje dotyczące wywołań interfejsu API aparatu, zadań i wyzwalaczy zadań, zadań dla gospodarstw domowych i tak dalej.
Agent replikacji programu DPM (DPMRA)	DPMRA	Rejestruje informacje na temat tworzenia kopii zapasowych na taśmach, replikacji dysku, przywracania oraz pomocniczych replikacji programu DPM. Na serwerze DPM i chronionym kliencie.
Agent biblioteki programu DPM (DPMLA)	LAAgent	Rejestruje działania dotyczące biblioteki. Na serwerze DPM i serwerze udostępnionej biblioteki.
Interfejs użytkownika programu DPM	DPMUI	Rejestruje działania interfejsu użytkownika, np. monitorowanie, ochronę, odzyskiwanie itp.
Interfejs wiersza polecenia PowerShell programu DPM	DPMCLI	Rejestruje wszystkie działania poleceń cmdlet
Menedżer dostępu programu DPM	DPMMAC	Rejestruje zachowanie automatyczne, np. zadania zwiększania, ponownego uruchamiania oraz informacje dotyczące Menedżera kontroli dostępu.

USŁUGA/PROCES	NAZWA PLIKU BINARNEGO	SZCZEGÓŁY
Otoka poleceń cmdlet programu Exchange Otoka E14 poleceń cmdlet	ExchangeCmdletsWrapper	Dzienniki różnych poleceń cmdlet uruchamianych przez program DPMRA po stronie klienta programu Exchange
Koordinator agenta	AgentBootStrapper	Rejestruje podczas instalacji i uaktualniania agenta
Usługa klienta programu DPM	DPMClientProtection	Dzienniki klientów programu DPM zainstalowanych na laptopach. Używany tylko po stronie laptopów.
Narzędzie kopii zapasowych programu DPM	DpmBackup	Dzienniki narzędzia wykonującego kopię zapasową programu DPM
Zainstaluj przygotowanie bazy SQL (zdalne przygotowanie bazy SQL)	Program inicjujący przygotowanie bazy SQL	Rejestruje podczas instalacji zdalnego serwera SQL przed uruchomieniem Instalatora.
Kopia zapasowa programu DPM	DpmBackup	Dzienniki narzędzia kopii zapasowej programu DPM
Edytor programu DPM	DPMWriter	Rejestruje podczas tworzenia kopii zapasowych na taśmach innych producentów i kopii zapasowych serwera pomocniczego. Tylko na serwerze DPM.
Otoka poleceń cmdlet programu WSS	WssCmdletsWrapper	Rejestruje podczas uruchamiania poleceń cmdlet programu WSS na froncie WFE programu SharePoint. Tylko na chronionym kliencie. Rejestruje w folderze: %USERPROFILE%\AppData\Roaming\Microsoft\Microsoft System Center Data ProtectionManager 2012\
Klient programu SQL EUR	EurClient	Zainstalowany na maszynach z zainstalowanym klientem SQL EUR. Rejestruje informacje na temat podłączania do serwera DPM, wyzwiania i anulowania operacji odzyskiwania itp. Rejestruje w folderze: %USERPROFILE%\AppData\Roaming\Microsoft\Microsoft System Center Data ProtectionManager 2012\

USŁUGA/PROCES	NAZWA PLIKU BINARNEGO	SZCZEGÓŁY
Interfejs użytkownika klienta przenośnego	DPMClientUI	Rejestruje różne działania wywoływane z poziomu interfejsu użytkownika klienta programu DPM i niepowodzenia. Rejestruje w folderze: %USERPROFILE%\AppData\Roaming\Microsoft\Microsoft System Center Data ProtectionManager 2012\

Generowanie raportów programu DPM

11.12.2019 • 33 minutes to read

Program System Center Data Protection Manager (DPM) używa SQL Server Reporting Services do tworzenia raportów. W obszarze zadania **Raportowanie** można wygenerować i wyświetlić raporty, zaplanować automatyczne generowanie raportów, zarządzać ustawieniami i subskrybować raporty. Można też wygenerować raporty programu DPM z programu Operations Manager, jeśli jest on używany do monitorowania programu DPM.

Raporty programu DPM

Program DPM oferuje różne rodzaje raportów:

- **Raport o stanie:** zawiera informacje o stanie wszystkich punktów odzyskiwania w określonym przedziale czasu. Zawiera on listę zadań odzyskiwania oraz łączną liczbę sukcesów i niepowodzeń dla punktów odzyskiwania i operacji tworzenia punktów odzyskiwania. Ten raport służy do śledzenia i sprawdzania metryk punktu odzyskiwania.
- **Raport dot. ochrony:** zawiera często używane metryki dotyczące pomyślnego utworzenia kopii zapasowych w długim okresie. Ten raport umożliwia śledzenie przebiegu tworzenia kopii zapasowych i sprawdzenie, co zostało zawarte w utworzonej kopii zapasowej.
- **Raport dot. odzyskiwania:** zawiera często używane metryki dotyczące pomyślnego odzyskiwania w długim okresie. Ten raport umożliwia śledzenie przebiegu operacji odzyskiwania i sprawdzenie jakości wykonania operacji względem Twojej umowy SLA pod kątem docelowego czasu odzyskiwania.
- **Raport wykorzystania dysku:** podsumowuje pojemność dysku, alokację dysku oraz użycie dysku w puli magazynu programu DPM. Ten raport umożliwia wykonanie następujących czynności: identyfikacja trendów wykorzystania dysku i podejmowanie decyzji o modyfikowaniu alokacji miejsca.
- **Raport dot. zarządzania taśmami i wykorzystania taśm:** raport dot. zarządzania taśmami służy do śledzenia informacji o rotacji i likwidowaniu taśm i do sprawdzania, czy nie został przekroczony próg wolnych nośników. Raport dot. wykorzystania taśm służy do śledzenia trendów dotyczących użycia zasobów (na dyskach lub taśmach) w czasie, ułatwiając planowanie pojemności.

Wstępnie zdefiniowane raporty SQL

Program DPM zawiera kilka widoków programu SQL Server ułatwiających tworzenie raportów niestandardowych. Widoki SQL zapewniają prostszą metodę niż bezpośrednio tabele kwerendy poprzez wypełnianie kolumn danymi zgromadzonymi z wielu tabel z bazy danych. Nie potrzebujesz dogłębnej znajomości całej bazy danych ani powiązania między tabelami i kluczami.

Z drugiej strony widoki SQL mogą obniżyć wydajność, jeśli są używane zbyt często, ponieważ widok za każdym razem uruchamia zapytania. Ponadto obsługiwane widoki mogą nie zawierać wszystkich potrzebnych kolumn.

Poniższa tabela zawiera podsumowanie wstępnie zdefiniowanych widoków SQL.

WIDOK	POLE	TYP DANYCH	OPIS
Vw_DPM_Agents Zawiera listę komputerów, na których jest zainstalowany agent ochrony programu DPM z tego serwera DPM.	ServerName	String	Nazwa komputera
Vw_DPM_Agents	Wersja	String	Wersja agenta programu DPM na tym komputerze
Vw_DPM_Alerts Lista alertów z ostatnich 30 dni	Ważność	Integer 0 = Błąd 1 = Ostrzeżenie 2 = Informacje	Ważność alertu
Vw_DPM_Alerts	Rozwiązanie	Integer 0 = Aktywny 1 = Zalecana akcja w toku 2 = Rozwiązany	Stan alertu
Vw_DPM_Alerts	OccurredSince	Data i godzina	Godzina, o której alert pojawił się po raz pierwszy
Vw_DPM_Alerts	ResolvedTime	Data i godzina	Godzina, o której alert został rozwiązany
Vw_DPM_Alerts	Typ	Integer	Typ alertu
Vw_DPM_CurrentOnlineMedia Taśmy będące obecnie w trybie online w bibliotekach należących do programu DPM według ostatniej inwentaryzacji.	UserFriendlyName	String	Nazwa biblioteki
Vw_DPM_CurrentOnlineMedia	ImportPoolMediaCount	Integer	Taśmy importowane na serwer DPM
Vw_DPM_CurrentOnlineMedia	FreePoolMediaCount	Integer	Taśmy oznaczone jako wolne lub puste
Vw_DPM_CurrentOnlineMedia	AdminPoolMediaCount	Integer	Taśmy z danymi aktywnymi

WIDOK	POLE	TYP DANYCH	OPIS
Vw_DPM_Disk_Usage_Repl ica Statystyka użycia dysku dla replik w puli magazynów.	PhysicalPath	String	Nazwa chronionego źródła danych
Vw_DPM_Disk_Usage_Repl ica	ReplicaId	Identyfikator GUID	Unikalny identyfikator repliki
Vw_DPM_Disk_Usage_Repl ica	PGId	Identyfikator GUID	Unikalny identyfikator grupy ochrony, do której należy źródło danych
Vw_DPM_Disk_Usage_Repl ica	ProductionServerName	String	Serwer, na którym znajduje się źródło danych
Vw_DPM_Disk_Usage_Repl ica	DiskAllocated	Duża liczba całkowita	Całkowite miejsce na dysku przydzielone do źródła danych
Vw_DPM_Disk_Usage_Repl ica	DiskUsed	Duża liczba całkowita	Całkowite miejsce na dysku używane przez źródło danych
Vw_DPM_Disk_Usage_Repl ica	FreeSpace	Duża liczba całkowita	DiskAllocated — DiskUsed
Vw_DPM_Disk_Usage_Repl ica	ReplicaAllocated	Duża liczba całkowita	Część DiskAllocated zarezerwowana dla repliki źródła danych
Vw_DPM_Disk_Usage_Repl ica	ReplicaUsed	Duża liczba całkowita	Część ReplicaAllocated rzeczywiście w użyciu
Vw_DPM_Disk_Usage_Repl ica	ShadowCopyAllocated	Duża liczba całkowita	Część DiskAllocated zarezerwowana dla punktów odzyskiwania źródła danych
Vw_DPM_Disk_Usage_Repl ica	ShadowCopyUsed	Duża liczba całkowita	Część ShadowCopyAllocated rzeczywiście w użyciu
Vw_DPM_Disk_Usage_Repl ica	StartDateTime	Data i godzina	
Vw_DPM_Disk_Usage_Repl ica	EndTime	Data i godzina	
Vw_DPM_Disk_Usage_Repl ica	ScheduleType	Integer 0 = co tydzień; 1 = co miesiąc; 2 = co kwartał; 3 = co rok	

WIDOK	POLE	TYP DANYCH	OPIS
Vw_DPM_DiskRecoveryPoints Liczniki punktów przywracania dysku dostępne dla każdego źródła danych.	DataSourceName	String	Nazwa chronionego źródła danych
Vw_DPM_DiskRecoveryPoints	PGId	Identyfikator GUID	Unikalny identyfikator grupy ochrony, do której należy źródło danych
Vw_DPM_DiskRecoveryPoints	ServerId	Identyfikator GUID	Unikalny identyfikator serwera, do którego należy źródło danych
Vw_DPM_DiskRecoveryPoints	Częstotliwość	Integer	Liczba dostępnych punktów odzyskiwania
Vw_DPM_LongRecoveries Informacje historyczne na temat procesów odzyskiwania, które trwały dłużej niż 24 godziny.	DataSourceName	String	Źródło danych, które zostało odzyskane
Vw_DPM_LongRecoveries	TargetServerName	String	Nazwa serwera, na który przeprowadzono odzyskiwanie
Vw_DPM_LongRecoveries	WriterId	Identyfikator GUID	Identyfikuje typ źródła danych, które zostało odzyskane
Vw_DPM_LongRecoveries	StartTime	Data i godzina	Godzina, o której zostało uruchomione odzyskiwanie
Vw_DPM_LongRecoveries	EndTime	Data i godzina	Godzina, o której zostało zakończone odzyskiwanie
Vw_DPM_Media Informacje dotyczące stanu wszystkich taśm rozpoznawanych przez program DPM.	MediaLabel	String	Etykieta na taśmie
Vw_DPM_Media	MediaBarcode	String	Kod kreskowy na taśmie
Vw_DPM_Media	IsOnline	Integer	Czy taśma jest w trybie online

WIDOK	POLE	TYP DANYCH	OPIS
Vw_DPM_Media	LibraryName	String	Nazwa biblioteki, w której znajduje się taśma. Wartość NULL, jeśli taśma jest w trybie offline
Vw_DPM_Media	MediaSlotNumber	Integer	Numer gniazda, w którym znajduje się taśma. Wartość NULL, jeśli taśma jest w trybie offline Jeśli w stacji, oznacza to gniazdo główne taśmy (do którego taśma wraca po odinstalowaniu).
Vw_DPM_Media	PGName	String	Nazwa grupy ochrony, w której znajduje się taśma
Vw_DPM_Media	MediaExpiryDate	Data i godzina	Godzina, o której wszystkie zestawy danych na tej taśmie wygasną. Może zawierać datę przeszłą lub wartość NULL, jeśli taśma jest wolna.
Vw_DPM_MediaPool_Media Liczniki taśm dla danej biblioteki.	LibraryName	String	Nazwa biblioteki
Vw_DPM_MediaPool_Media	FreeMedia	Integer	Liczba taśm, które są wolne w tej bibliotece
Vw_DPM_MediaPool_Media	FreeMediaThreshold	Integer	Próg, poniżej którego ta biblioteka generuje alert
Vw_DPM_ProtectedDataSource Bieżące użycie miejsca na dysku przez różne źródła danych.	ReplicaId	Identyfikator GUID	Identyfikator repliki
Vw_DPM_ProtectedDataSource	PGId	Identyfikator GUID	Identyfikator grupy ochrony, do której należy replika
Vw_DPM_ProtectedDataSource	AllocatedSize	Duża liczba całkowita	Ilość miejsca na dysku przydzielona do źródła danych
Vw_DPM_ProtectedDataSource	UsedSize	Duża liczba całkowita	Ilość miejsca na dysku używana obecnie przez źródło danych

WIDOK	POLE	TYP DANYCH	OPIS
Vw_DPM_ProtectedDataS ource	ProductionServerName	String	Nazwa komputera, na którym znajduje się źródło danych
Vw_DPM_ProtectedDataS ource	StorageNode	String	Zawsze ustawione na serwer DPM
Vw_DPM_ProtectedGroup Tabela z informacjami o wszystkich grupach ochrony.	PGId	Identyfikator GUID	Unikalny identyfikator grupy ochrony
Vw_DPM_ProtectedGroup	ProtectionGroupName	String	Nazwa grupy ochrony
Vw_DPM_ProtectedGroup	CreationTime	Data i godzina	Godzina, o której utworzono grupę ochrony
Vw_DPM_RecoveryDuratio n Historia liczników dla zadań odzyskiwania w różnych okresach czasu.	StartDateTime	Data i godzina	Godzina, o której zostały zgromadzone dane statystyczne
Vw_DPM_RecoveryDuratio n	EndTime	Data i godzina	Wewnętrzna
Vw_DPM_RecoveryDuratio n	ScheduleType	Integer	Częstotliwość, dla której zostały zgromadzone te konkretne dane statystyczne
Vw_DPM_RecoveryDuratio n	RecoveryDuration	Integer	Wskazuje, czy odzyskiwanie trwało mniej niż 6 godzin, od 6 do 24 godzin czy dłużej niż 24 godziny
Vw_DPM_RecoveryDuratio n	RecoveryCount	Integer	Liczba operacji odzyskiwania
Vw_DPM_RecoveryJob Szczegółowe informacje dotyczące ostatnich zadań odzyskiwania.	DataSourceName	String	Źródło danych, dla którego zostało uruchomione odzyskiwanie
Vw_DPM_RecoveryJob	ServerName	String	Serwer, na który zostało wykonane odzyskiwanie
Vw_DPM_RecoveryJob	CreationTime	Data i godzina	Godzina, o której zostało uruchomione zadanie odzyskiwania
Vw_DPM_RecoveryJob	FailureCode	Integer	Kod błędu w przypadku niepowodzenia zadania odzyskiwania

WIDOK	POLE	TYP DANYCH	OPIS
Vw_DPM_RecoveryJob	Stan	Integer 0/1 = Postęp 2 = Powiodło się 3 = Niepowodzenie	Stan zadania odzyskiwania
Vw_DPM_RecoveryPointDisk Stan ostatnich zadań tworzenia punktów odzyskiwania na dysku.	String	Źródło danych, dla którego utworzono kopię zapasową	String
Vw_DPM_RecoveryPointDisk	String	Serwer, na którym znajduje się źródło danych	String
Vw_DPM_RecoveryPointDisk	Data i godzina	Godzina, o której zostało uruchomione zadanie tworzenia punktu odzyskiwania	Data i godzina
Vw_DPM_RecoveryPointDisk	Integer 0/1 = Postęp 2 = Powiodło się 3 = Niepowodzenie	Stan zadania tworzenia punktu odzyskiwania	Integer 0/1 = Postęp 2 = Powiodło się 3 = Niepowodzenie
Vw_DPM_RecoveryPointDisk	Integer	Zero, jeśli zakończyło się pomyślnie. W przeciwnym wypadku ustaw na kod błędu programu DPM.	Integer
Vw_DPM_RecoveryPointTape Stan ostatnich zadań tworzenia punktu odzyskiwania na taśmie.			
Vw_DPM_RecoveryPointTape	String	Źródło danych, dla którego utworzono kopię zapasową	String
Vw_DPM_RecoveryPointTape	String	Serwer, na którym znajduje się źródło danych	String
Vw_DPM_RecoveryPointTape	Data i godzina	Godzina, o której zostało uruchomione zadanie tworzenia punktu odzyskiwania	Data i godzina

WIDOK	POLE	TYP DANYCH	OPIS
Vw_DPM_RecoveryPointTape	Integer 0/1 = Postęp 2 = Powiodło się 3 = Niepowodzenie	Stan zadania tworzenia punktu odzyskiwania	Integer 0/1 = Postęp 2 = Powiodło się 3 = Niepowodzenie
Vw_DPM_Replica Lista wszystkich replik zarządzanych w programie DPM	ReplicaId	Identyfikator GUID	Unikalny identyfikator generowany w programie DPM dla woluminu repliki
Vw_DPM_Replica	PhysicalPath	String	Nazwa źródła danych repliki
Vw_DPM_Replica	ServerName	String	Nazwa serwera, do którego należy źródło danych
Vw_DPM_Replica	ValidFrom	Data i godzina	Data i godzina utworzenia repliki
Vw_DPM_Replica	ValidTo	Data i godzina	Dzień, w którym replika stała się nieaktywna
Vw_DPM_Replica	PGId	Identyfikator GUID	Unikalny identyfikator generowany w programie DPM dla grupy ochrony, do której należy źródło danych
Vw_DPM_Replica	StorageNode	String	Zawsze ustawione na serwer DPM
Vw_DPM_Server Lista wszystkich komputerów chronionych.	ServerId	Identyfikator GUID	Unikalny identyfikator generowany w programie DPM dla chronionego komputera
Vw_DPM_Server	ServerName	String	W pełni kwalifikowana nazwa domeny dla komputera
Vw_DPM_Server	NetBiosName	String	Nazwa
Vw_DPM_Server	DomainName	String	Domena, do której należy komputer
Vw_DPM_Server	IsRG	Integer	Czy ten komputer reprezentuje grupę zasobów

WIDOK	POLE	TYP DANYCH	OPIS
Vw_DPM_TapeRecoveryPoints Liczniki punktów odzyskiwania na taśmie dostępnych dla każdego źródła danych.	DataSourceName	String	Nazwa chronionego źródła danych
Vw_DPM_TapeRecoveryPoints	PGId	Identyfikator GUID	Unikalny identyfikator grupy ochrony, do której należy to źródło danych
Vw_DPM_TapeRecoveryPoints	ServerId	Identyfikator GUID	Unikalny identyfikator serwera, do którego należy to źródło danych
Vw_DPM_TapeRecoveryPoints	Częstotliwość	Integer	Liczba dostępnych punktów odzyskiwania
Vw_DPM_TapeRecoveryPoints	Termin	Integer 0 = Krótki; 1 = Długi	Harmonogram, któremu odpowiada punkt odzyskiwania
Vw_DPM_TapeStat Informacje historyczne na temat liczników użycia taśm.	StartDateTime	Data i godzina	
Vw_DPM_TapeStat	EndTime	Data i godzina	
Vw_DPM_TapeStat	ScheduleType	Integer	Integer 0 = Co tydzień 1 = Co miesiąc 2 = Co kwartał 3 = Co rok
Vw_DPM_TapeStat	Wolne	Integer	Liczba wolnych taśm w momencie zakończenia
Vw_DPM_TapeStat	W trybie online	Integer	Liczba taśm w trybie online w momencie zakończenia
Vw_DPM_TapeUsagePerPG Dane historyczne użycia taśmy na grupę ochrony.	StartDateTime	Data i godzina	Godzina rozpoczęcia
Vw_DPM_TapeUsagePerPG	EndTime	Data i godzina	Godzina zakończenia

WIDOK	POLE	TYP DANYCH	OPIS
Vw_DPM_TapeUsagePerPG	PGName	String	Nazwa grupy ochrony
Vw_DPM_TapeUsagePerPG	ScheduleType	Integer	Integer 0 = Co tydzień 1 = Co miesiąc 2 = Co kwartał 3 = Co rok
Vw_DPM_TapeUsagePerPG	W trybie online	Integer	Liczba taśm w trybie online w momencie zakończenia
Vw_DPM_TapeUsagePerPG	W trybie offline	Integer	Liczba taśm w trybie offline w momencie zakończenia
Vw_DPM_Total_Disk_Trend Trend historyczny dotyczący całkowitego użycia miejsca na dysku.	StartDateTime	Data i godzina	
Vw_DPM_Total_Disk_Trend	EndDateTime	Data i godzina	
Vw_DPM_Total_Disk_Trend	ScheduleType	Integer	Integer 0 = Co tydzień 1 = Co miesiąc 2 = Co kwartał 3 = Co rok
Vw_DPM_Total_Disk_Trend	DiskSpaceCapacity	Duża liczba całkowita	Całkowita ilość miejsca do magazynowania w puli magazynów w momencie zakończenia
Vw_DPM_Total_Disk_Trend	PreviousDiskSpaceCapacity	Duża liczba całkowita	Całkowita ilość miejsca do magazynowania w puli magazynów w poprzednim odpowiadającym okresie
Vw_DPM_Total_Disk_Trend	DiskSpaceAllocated	Duża liczba całkowita	Ilość miejsca na dysku z puli magazynów, która została przydzielona
Vw_DPM_Total_Disk_Trend	PreviousDiskSpaceAllocated	Duża liczba całkowita	Miejsce na dysku z puli magazynów, które zostało przydzielone w poprzednim odpowiadającym okresie

WIDOK	POLE	TYP DANYCH	OPIS
Vw_DPM_Total_Disk_Trend	DiskSpaceUsed	Duża liczba całkowita	Rzeczywiste użycie miejsca na dysku
Vw_DPM_Total_Disk_Trend	PreviousDiskSpaceUsed	Duża liczba całkowita	Użyte miejsce na dysku w poprzednim odpowiadającym okresie
Vw_DPM_Total_RecoveryPoint Informacje o wszystkich ostatnich zadaniach punktu odzyskiwania.	DataSourceName	String	Nazwa chronionego źródła danych
Vw_DPM_Total_RecoveryPoint	ServerName	String	Serwer, do którego należy źródło danych
Vw_DPM_Total_RecoveryPoint	CreationTime	Data i godzina	Godzina, o której zostało uruchomione zadanie tworzenia punktu odzyskiwania
Vw_DPM_Total_RecoveryPoint	Stan	Integer 0/1 = Postęp 2 = Powiodło się 3 = Niepowodzenie	Stan zadania tworzenia punktu odzyskiwania
Vw_DPM_Total_RecoveryPoint	ErrorCode	Integer	Kod błędu w operacji tworzenia punktu odzyskiwania

Konfigurowanie raportów

Planowanie raportów

Domyślnie w programie DPM raporty nie są zaplanowane. Aby rozpocząć tworzenie i zapisywanie raportów historycznych, należy utworzyć harmonogram raportów. Każdy typ raportu ma niezależny harmonogram. Każdy raport ma tylko jeden harmonogram. Zaplanuj raport w następujący sposób:

1. W konsoli administratora programu DPM przejdź do widoku **Raportowanie**. W okienku wybierz raport, a następnie kliknij przycisk **Harmonogram**.
2. Wybierz opcję **Uruchom raport zgodnie z opcjami harmonogramu**.
3. Na karcie **Harmonogram** wybierz opcje harmonogramu, w tym częstotliwość, sposób grupowania, godzinę generowania oraz stopień szczegółowości. Stopień szczegółowości jest ograniczony przez częstotliwość. W związku z tym jeśli częstotliwość wynosi tydzień, taki sam jest stopień szczegółowości. Dotyczy to również okresu czasu objętego raportem i liczby kopii do przechowania w historii.

Wyświetlanie raportów

Konsola administratora programu DPM umożliwia wyświetlanie nowych i historycznych raportów w programie Internet Explorer. Aby dostosować, wyeksportować lub wydrukować raport, można skorzystać z paska narzędzi usług sieci Web programu Reporting Services znajdującego się w górnej części raportu.

1. W celu utworzenia nowego raportu można wybrać następujące ustawienia:

- Wyświetl — wyświetlanie grup raportów według chronionego komputera lub grupy ochrony.
 - Można wybrać lub wykluczyć określony przedział czasowy. Poziom szczegółowości raportu można ustawić w następujący sposób:
 - Tydzień — 7 dni, od niedzieli do soboty
 - Miesiąc — pełny miesiąc, od pierwszego do ostatniego dnia miesiąca
 - Co kwartał — trzy miesiące, począwszy od stycznia (np. od stycznia do marca).
 - Co rok — od 1 stycznia do 31 grudnia danego roku.
2. Dostępny raport do wyświetlenia można wybrać z listy **Dostępne raporty**. Jeśli liczba zapisanych raportów historycznych jest równa maksymalnej liczbie określonej w harmonogramie raportu, kolejny zapisany raport zastępuje najstarszą kopię raportu. Dzięki temu przez cały czas można zachowywać maksymalną liczbę kopii.

Drukowanie raportów

Raporty programu DPM są przeznaczone do drukowania w formacie A4 bez poziomego podziału informacji na stronach. Edycja formatów MHTML i PDF jest niemożliwa, dlatego nie można modyfikować raportu tak, aby dopasować go do innych rozmiarów papieru.

Należy pamiętać, że jeśli występują problemy związane z dopasowywaniem raportów do formatu A4, należy spróbować zmienić wymiary strony raportu (szerokość 210 mm i wysokość 297 mm). Szczegółowe informacje na ten temat można znaleźć w blogu Boba Cornelissena: [Blog BICTT](#).

Drukowanie raportów MHTML

1. W menu **Plik** programu Internet Explorer kliknij polecenie **Ustawienia strony**.
2. Ustaw rozmiar papieru na A4 i wybierz pozycję **Orientacja > Pionowa**.
3. Ustaw opcję **Marginesy** na wartości nieprzekraczające następujących wielkości (w milimetrach): **Lewy: 2,8, Prawy: 2,8, Górny: 2,8, Dolny: 2,8**. Następnie wydrukuj raport.

Drukowanie raportu w formacie PDF

1. W programie Adobe Acrobat otwórz okno dialogowe **Drukowanie**.
2. Ustaw opcję **Skalowanie strony** na **Zmniejszanie dużych stron** (ustawienie domyślne). Wybierz opcję **Automatyczne obracanie i środkowanie**.
3. Na karcie **Zaawansowane** ustaw orientację na **Pionowa** i wydrukuj raport.

Drukowanie raportu za pomocą programu Microsoft Excel

1. Otwórz plik w programie Excel.
2. Kliknij przycisk **Układ strony > Orientacja > Pionowa**.
3. Kliknij pozycję **Rozmiar > A4**.
4. Kliknij pozycję **Marginesy > Marginesy niestandardowe**. Ustaw marginesy (**Górny, Lewy, Dolny**) oraz opcję **Stopka** na wartość 0.
5. W obszarze **Skaluj do rozmiaru** ustaw wartość pola **Skala** na 80%.
6. W obszarze **Opcje arkusza** usuń ewentualne zaznaczenie pola wyboru **Drukuj**. Następnie wydrukuj raport.

Wysyłanie raportów

Raporty można wysyłać do subskrybentów w wiadomościach e-mail. Raporty są wysyłane jako załączone pliki. Aby subskrybować raporty:

1. Wskaż serwer SMTP, który ma być używany przez program DPM do wysyłania raportów.
2. W widoku Raportowanie w okienku wyświetlania kliknij prawym przyciskiem myszy raport, który chcesz

subskrybować, i kliknij przycisk **Harmonogram**.

3. Na karcie **E-mail** w polu **Adresaci** wprowadź adresy e-mail wszystkich subskrybentów. Dodaj tylko adresatów związanych z wybranym serwerem. Adresy e-mail rozdziel przecinkami. Następnie wybierz format.

Generowanie raportów programu DPM w programie Operations Manager

W programie Operations Manager są dostępne konsola Operacje oraz konsola sieci Web, które umożliwiają wyświetlanie i przetwarzanie danych monitorowania dotyczących środowiska użytkownika. Aby pobrać informacje, można użyć wstępnie zdefiniowanych widoków lub wyszukiwać dane i obiekty przy użyciu funkcji wyszukiwania i filtrowania. Aby uzyskać więcej informacji, zobacz [Uzyskiwanie informacji z programu Operations Manager](#). Program DPM udostępnia wiele wstępnie zdefiniowanych widoków, których można użyć do wyszukiwania, co jest prostsze niż definiowanie własnych zapytań lub filtrów.

Program DPM udostępnia wiele wstępnie zdefiniowanych widoków, których można użyć do wyszukiwania, co jest prostsze niż definiowanie własnych zapytań lub filtrów.

Nazwa widoku: vDPMBackupJob (pokazuje szczegóły zadania kopii zapasowej):

POLE	TYP DANYCH	OPIS
BackupJobRowId	uniqueidentifier	Klucz indeksu
DPMServerName	varchar(max)	Serwer programu DPM
TaskID	uniqueidentifier	Identyfikator zadania unikatowo określający zadanie
VerbID	uniqueidentifier	Określa typ zadania
ProtectionServer	varchar(max)	Serwer ochrony lub klaster, dla którego uruchomiono zadanie
ProtectionGroupID	uniqueidentifier	Identyfikator grupy ochrony, dla którego uruchomiono zadanie
ProtectionGroup	varchar(max)	Nazwa grupy ochrony
DataSourceID	uniqueidentifie	Identyfikator źródła danych, dla którego uruchomiono zadanie
DataSourceName	varchar(max)	Nazwa źródła danych
StartedDateTime	datetime	Godzina rozpoczęcia zadania
StoppedDateTime	datetime	Godzina zakończenia zadania
ExecutionState	int	2 = powiodło się; 3 = nie powiodło się
ErrorCode	int	Kod błędu zadania zakończonego niepowodzeniem. Kod błędu można zignorować, jeśli zadanie zakończyło się pomyślnie.

POLE	TYP DANYCH	OPIS
ErrorString	varchar(max)	Odpowiedni zlokalizowany ciąg błędu
TransferredBytes	int	Liczba bajtów przesłanych w ramach zadania
BackupType	varchar(max)	DiskBackup (kopia zapasowa na dysku); TapeBackup (kopia zapasowa na taśmie); CloudBackUp (kopia zapasowa w chmurze)
IsDPM	bit	Określa, czy zadanie zostało wykonane na serwerze DPM (wskazuje, że zostało wykonane na pomocniczym serwerze programu DPM)
IsAdHoc	bit	Określa, czy jest to zadanie ad hoc, czy też wykonywane według harmonogramu

Nazwa widoku: vDPMRecoveryJob (szczegóły zadania odzyskiwania):

POLE	TYP DANYCH	OPIS
RecoveryJobRowID	uniqueidentifier	Klucz indeksu
DPMServerName	varchar(max)	Serwer programu DPM
TaskID	uniqueidentifier	Identyfikator zadania unikatowo określający zadanie
DataSourceID	uniqueidentifier	Identyfikator źródła danych, dla którego uruchomiono zadanie odzyskiwania
DataSourceName	varchar(max)	Źródło danych, dla którego uruchomiono zadanie odzyskiwania
StartedDateTime	datetime	Godzina rozpoczęcia zadania
StoppedDateTime	datetime	Godzina zakończenia zadania
ExecutionState	Int	2 = zakończyło się pomyślnie; 3 = nie powiodło się
ErrorCode	int	Kod błędu. Ten błąd należy zignorować w przypadku pomyślnego zakończenia zadania.
ErrorString	varchar(max)	Odpowiedni zlokalizowany ciąg błędu
TransferredBytes	int	Liczba bajtów przesłanych w ramach zadania
RecoverySource	int	0 = dysk; 1 = taśma; 2 = chmura

POLE	TYP DANYCH	OPIS
RecoveryType	int	Wskazuje typ odzyskiwania
TargetServerName	varchar(max)	Serwer docelowy, na którym zostało wykonane odzyskiwanie
TargetLocation	varchar(max)	Ścieżka folderu, na której zostało wykonane odzyskiwanie
IsExternalSource	int	Wskazuje, czy źródło danych jest zewnętrzne (na przykład z taśmy zaimportowanej z innego serwera DPM)

Nazwa widoku: vDPMDiskManagement (wyświetla informacje dotyczące zarządzania dyskiem):

POLE	TYP DANYCH	OPIS
DiskManagementRowID	uniqueidentifier	Klucz indeksu
DPMServerName	varchar(max)	Serwer programu DPM
DiskID	uniqueidentifier	Unikatowy identyfikator dysku
DiskName	varchar(max)	Nazwa dysku zwracana przez interfejsy API usługi VDS (na przykład „Microsoft Virtual Disk”)
TotalSize	bigint	Całkowity rozmiar dysku
FreeSize	bigint	Rozmiar wolnego miejsca na dysku
IsInStoragePool	bit	Wskazuje, czy dysk należy do puli magazynów programu DPM
DiskType	smallint	0 = podstawowy, 1 = dynamiczny; 2 = niezainicjowany
HealthStatus	smallint	0 = w dobrej kondycji; 1 = uszkodzony
IsMissing	bit	Wskazuje brak dysku
IsForeign	bit	Wskazuje, czy dysk jest obcy
CanAddToStoragePool	bit	Wskazuje, czy dysk może zostać dodany do puli magazynów programu DPM
CreatedDateTime	datetime	Godzina utworzenia

Nazwa widoku: vDPMDiskUtilization (pokazuje statystyki dysku):

POLE	TYP DANYCH	OPIS
DiskUtilizationRowID	uniqueidentifier	Klucz indeksu

POLE	TYP DANYCH	OPIS
DPMServerName	varchar(max)	Serwer programu DPM
SMStatsID	uniqueidentifier	Wewnętrzny identyfikator statystyk używany przez program DPM
DataSourceID	uniqueidentifier	Identyfikator źródła danych, dla którego uruchomiono zadanie
DataSourceName	varchar(max)	Źródło danych, dla którego uruchomiono zadanie
ProductionServer	varchar(max)	Serwer lub klaster, do którego należy źródło danych
ProtectionGroupID	uniqueidentifier	Identyfikator grupy ochrony, do której należy źródło danych
ProtectionGroup	varchar(max)	Nazwa grupy ochrony, do której należy źródło danych
ReplicaSpaceAllocated	bigint	Całkowity rozmiar woluminu repliki
ShadowCopyAllocatedSize	bigint	Rozmiar woluminu kopii w tle
ShadowCopyUsedSize	bigint	Używany rozmiar woluminu kopii w tle
ReplicaUsedSize	bigint	Używany rozmiar woluminu repliki
FreeSpaceAvailable	bigint	Całkowite wolne miejsce na woluminach repliki i kopii w tle
IsCollocated	int	Wskazuje, czy wolumin jest używany dla kolokowanej grupy ochrony, która może mieć wiele źródeł danych

Nazwa widoku: vDPMSLATrend (przydaje się do wyświetlania wartości procentowej wystąpień spełniających — lub nie — umowę SLA):

POLE	TYP DANYCH	OPIS
SLATrendRowId	uniqueidentifier	Klucz indeksu
DPMServerName	varchar(max)	Serwer programu DPM
SMStatsID	uniqueidentifier	Identyfikator statystyk używany w programie DPM
StartTime	datetime	Rozpoczęcie określonego okresu umowy SLA
EndTime	datetime	Zakończenie określonego okresu umowy SLA

POLE	TYP DANYCH	OPIS
DataSourceID	uniqueidentifier	Identyfikator źródła danych, dla którego uruchomiono zadanie
DatasourceName	varchar(max)	Nazwa źródła danych, dla którego uruchomiono zadanie
ProtectionServer	varchar(max)	Serwer lub klaster, do którego należy źródło danych
ProtectionGroupID	uniqueidentifier	Identyfikator grupy ochrony, do której należy źródło danych
ProtectionGroupName	varchar(max)	Grupa ochrony, do której należy źródło danych
CreationTime	datetime	Godzina utworzenia statystyki
DiskRecoveryPointAvailable	bit	Wskazuje, czy w okresie umowy SLA jest dostępny punkt odzyskiwania z dysku
TapeRecoveryPointAvailable	bit	Wskazuje, czy w okresie umowy SLA jest dostępny punkt odzyskiwania z taśmy
CloudRecoveryPointAvailable	bit	Wskazuje, czy w okresie umowy SLA jest dostępny punkt odzyskiwania z chmury
umowa SLA	int	Wskazuje umowę SLA dla grupy ochrony w trakcie tego okresu umowy SLA

Nazwa widoku: vDPMTapeUtilization (pokazuje wykorzystanie taśmy DPM):

POLE	TYP DANYCH	OPIS
TapeUtilizationRowId	uniqueidentifier	Klucz indeksu
DPMServerName	varchar(max)	Serwer programu DPM
SMStatsID	uniqueidentifier	Unikatowy identyfikator statystyk w programie DPM
StartTime	datetime	Rozpoczęcie okresu statystyk
EndTime	datetime	Zakończenie okresu statystyk
FreeTapeCount	int	Liczba wolnych taśm dołączonych do serwera DPM
OnlineTapeCount	int	Liczba taśm online dołączonych do serwera DPM
OfflineTapeCount	int	Liczba taśm offline dołączonych do serwera DPM

Nazwa widoku: vDPMTapeManagement (przedstawia informacje programu DPM dotyczące bibliotek taśm i identyfikacji taśm):

POLE	TYP DANYCH	OPIS
TapeManagementRowID	uniqueidentifier	Klucz indeksu
DPMServerName	varchar(max)	Serwer programu DPM
MediaSlotNumber	int)	Numer gniazda biblioteki, w którym znajduje się nośnik
MediaBarcode	varchar(max)	Kod kreskowy taśmy
MediaLabel	varchar(max)	Etykieta taśmy
IsOnline	bit	Wskazuje, czy taśma jest w trybie online
LibraryName	varchar(max)	Nazwa biblioteki
ProtectedGroupName	varchar(max)	Nazwa grupy ochrony będącej właścicielem taśmy
MediaExpiryDate	datetime	Data wygaśnięcia taśmy

Zarządzanie i monitorowanie serwerów DPM przy użyciu programu Operations Manager

11.12.2019 • 7 minutes to read

Konsola centralna to konsola System Center Operations Manager, którą można wdrożyć w celu zarządzania wieloma serwerami programu System Center Data Protection Manager (DPM) i ich monitorowania z jednej lokalizacji. Umożliwia ona:

- Scentralizowane monitorowanie serwerów DPM z jednej lokalizacji — można monitorować różne wersje programu DPM oraz śledzić stan i kondycję serwerów, zadań, zasobów chronionych, bibliotek taśm, dostępnej pamięci i miejsca na dysku oraz kopii zapasowych.
- Alerty oparte na umowie dotyczącej poziomu usług (SLA). Alerty są generowane w przypadku naruszenia postanowień umowy SLA.
- Wyświetlanie stanu wszystkich ról na serwerach programu DPM.
- Monitorowanie, identyfikowanie, działanie i rozwiązywanie problemów z alertami wygenerowanymi w przypadku przerwania umowy SLA. Alerty można skonsolidować, aby pokazać:
 - tylko jedno wystąpienie dla powtórzonych alertów;
 - pojedynczy alert dotyczący alertów o tej samej głównej przyczynie lub jeśli wiele kopii zapasowych nie powiedzie się dla tego samego źródła danych,
 - i Generuj tylko jeden bilet, jeśli jest używany system biletów
- Zdalne akcje naprawcze i zdalne odzyskiwanie.
- Monitorowanie pamięci serwera programu DPM, procesora, zasobów dysku, bazy danych i trendów wydajności
- Modyfikowanie ustawień i zarządzanie nimi, w tym przydzielanie dysku, punkty odzyskiwania, użytkownicy, ochrona grup
- Odzyskiwanie danych

Konfigurowanie programu Central Console

Wymagane elementy:

- Serwer System Center Operations Manager z systemem 2016. Magazyn danych programu Operations Manager musi być uruchomiony i działać prawidłowo.
- Wyświetlanie stanu wszystkich ról na serwerach programu DPM.
- Aby można było zainstalować pakiety administracyjne, na serwerze DPM musi być uruchomiony program DPM 2012 R2 z pakietem zbiorczym aktualizacji 5 lub DPM 2016.
- Jeśli uruchomiona jest wcześniejsza wersja pakietów administracyjnych odnajdowania i biblioteki uzyskana z nośnika instalacyjnego programu DPM, należy usunąć je z serwera programu DPM i zainstalować nowe wersje ze strony pobierania.
- Można uruchamiać tylko jedną wersję językową pakietu administracyjnego naraz. Aby użyć pakietu w innym języku, należy odinstalować pakiet w istniejącym języku, a następnie zainstalować go w nowym języku.

Konsolę centralną należy wdrożyć w następujący sposób:

1. [Zainstaluj agenta programu Operations Manager](#) — zainstaluj agenta programu Operations Manager na każdym serwerze DPM, który ma być monitorowany i zarządzany.
2. [Zaimportuj pakiety administracyjne odnajdowania i biblioteki](#) — pobierz pakiety i zainstaluj je na serwerze programu Operations Manager.

3. [Zainstaluj program Central Console](#) — zainstaluj program Central Console na serwerze programu Operations Manager.
4. [Zainportuj pakiet administracyjny raportowania programu DPM](#) — pobierz pakiet i zainstaluj go na serwerze programu Operations Manager.

Instalacja agenta programu Operations Manager

Zainstaluj agenta w następujący sposób:

1. Zainstaluj agenta na każdym serwerze programu DPM, który chcesz monitorować.
2. [Pobierz](#) najnowszą wersję agenta.

Importowanie pakietów administracyjnych odnajdywania i biblioteki programu DPM

Program DPM zapewnia następujące pakiety administracyjne:

- Pakiet administracyjny raportowania (Microsoft.SystemCenter.DataProtectionManager.2012.Reporting.mp) — gromadzi i wyświetla dane raportowania z wszystkich serwerów programu DPM i ujawnia zestaw widoków magazynu programu Operations Manager dla programu DPM. Można tworzyć zapytania dotyczące tych widoków, aby generować raporty niestandardowe.
- Pakiet administracyjny odnajdywania i monitorowania (Microsoft.SystemCenter.DataProtectionManager.2012.Discovery.mp)
- Pakiet administracyjny biblioteki — (Microsoft.SystemCenter.DataProtectionManager.2012.Library)

1. Na serwerze Operations Manager Usuń wszystkie istniejące pakiety administracyjne programu DPM.
2. [Pobierz](#) pakiety administracyjne programu DPM.

Domyślnie pobrane pakiety administracyjne odnajdywania i biblioteki są umieszczane w folderze C:\Program Files\System Center Management Packs. Pakiet administracyjny raportowania jest umieszczany w oddzielnym folderze wewnątrz tego folderu.

3. Zaloguj się do serwera programu Operations Manager za pomocą konta, które jest elementem członkowskim roli Administratorzy programu Operations Manager.
4. Pamiętaj, aby usunąć wszystkie poprzednie wersje pakietów administracyjnych biblioteki lub odnajdywania działające na serwerze.
5. W konsoli Operacje kliknij pozycję **Administracja**. Kliknij prawym przyciskiem myszy pozycję **Pakiety administracyjne > Importuj pakiety administracyjne**.
6. Wybierz pozycję **Microsoft.SystemCenter.DataProtectionManagerDiscovery.MP > Otwórz**, a następnie pozycję **Microsoft.SystemCenter.DataProtectionManagerLibrary.MP > Otwórz**.
7. Postępuj zgodnie z instrukcjami kreatora Importowanie pakietów administracyjnych.

Instalowanie programu Central Console

1. Wybierz opcję **Zainstaluj składniki serwerowe i klienckie programu Central Console**, jeśli chcesz monitorować serwery DPM, na których jest zainstalowany agent programu Operations Manager i uruchamiać konsolę administratora programu DPM na serwerze programu Operations Manager.
2. Wybierz opcję **Zainstaluj składniki serwerowe programu Central Console**, jeśli chcesz tylko monitorować serwery bez korzystania z konsoli administratora programu DPM.

Należy pamiętać o następujących kwestiach:

- Program DPM dodaje wyjątki zapory dla portu 6075, aby umożliwić komunikację konsoli administratora z zakresami. Należy otworzyć porty dla programów SQL Server.exe i SQL browser.exe.

- Jeśli musisz odinstalować program Operations Manager, zapoznaj się z tematem [Jak odinstalować program Operations Manager](#).

Importowanie pakietu administracyjnego raportowania

1. Zaloguj się do serwera programu Operations Manager za pomocą konta, które jest elementem członkowskim roli Administratorzy programu Operations Manager.
2. W konsoli Operacje kliknij pozycję **Administracja**. Kliknij prawym przyciskiem myszy pozycję **Pakiety administracyjne > Importuj pakiety administracyjne**.
3. Wybierz pozycję **Microsoft.SystemCenter.DataProtectionManagerReporting.MP > Otwórz**.
4. Postępuj zgodnie z instrukcjami kreatora Importowanie pakietów administracyjnych.

Następne kroki

Po zaimportowaniu pakiety administracyjne odnajdują i monitorują dane bez konieczności dodatkowej konfiguracji. Można opcjonalnie dostosować ustawienia, takie jak monitory i reguły dla danego środowiska. Na przykład jeśli okaże się, że włączone zasady pomiaru wydajności obniżają wydajność serwerów mających wolne łącza sieci WAN, można je wyłączyć. Gdy wszystko jest skonfigurowane jako potrzebne, można generować raporty programu DPM z Operations Manager.

Poprawianie wydajności replikacji

11.12.2019 • 6 minutes to read

Aby zoptymalizować wydajność replikacji i synchronizacji danych programu System Center 2012 — Data Protection Manager (DPM), możesz podjąć kilka kroków, w tym ograniczyć przepustowość sieci, włączyć kompresję danych, zróżnicować godziny rozpoczęcia synchronizacji i zoptymalizować ekspresowe tworzenie kopii zapasowych.

Ograniczanie przepustowości sieci

Konfiguracji ograniczenia przepustowości sieci można dokonać z poziomu maszyny, dla której wykonano kopię zapasową, oraz można określić różne wartości ograniczenia przepustowości w godzinach pracy, godzinach wolnych i w weekendy. Dla każdej z tych kategorii można określić zakres godzin. Włącz ograniczanie w następujący sposób:

1. Otwórz konsolę programu DPM i wybierz pozycję **Zarządzanie > Agent**, wybierz maszynę, na której chcesz ograniczyć przepustowość i wybierz opcję **Ogranicz przepustowość**.
2. Kliknij pozycję **Ogranicz przepustowość > Włącz ustawienie ograniczenia przepustowości**.
3. Dla maszyny wybierz opcje **Ustawienia ograniczania przepustowości** i **Harmonogram pracy**, a następnie kliknij przycisk **OK**.

NOTE

Można skonfigurować osobno ograniczanie przepustowości sieci podczas godzin pracy i po godzinach oraz zdefiniować godziny pracy dla komputera chronionego.

4. Aby zastosować ustawienia, kliknij przycisk **OK**.

Warto zauważyć, że wykorzystanie przepustowości sieci można również ograniczyć, używając zasad grupy.

Limit przepustowości określony przez zasady grupy na komputerze lokalnym określa łączną przepustowość dla wszystkich programów używających harmonogramu pakietów, w tym dla programu DPM. Limit wykorzystania przepustowości sieci przez program DPM określa przepustowość sieci wykorzystywaną przez program DPM podczas tworzenia repliki, synchronizacji oraz sprawdzania spójności.

Jeśli limit wykorzystania przepustowości programu DPM, samodzielnie lub w połączeniu z wartościami granicznymi innych programów, przekracza limit przepustowości zasad grupy, limit wykorzystania przepustowości programu DPM może zostać niewykorzystany. Na przykład jeśli komputer DPM z połączeniem sieciowym o przepustowości 1 gigabit na sekundę (Gb/s) ma limit przepustowości zasad grupy równy 20%, wówczas 200 Mb/s przepustowości jest zarezerwowane dla wszystkich programów, które używają harmonogramu pakietów. Jeśli przepustowość programu DPM zostanie następnie ustawiona na wartość maksymalną 150 Mb/s, podczas gdy wykorzystanie przepustowości przez usługi Internet Information Services (IIS) ma wartość maksymalną 100 Mb/s, łączne limity użycia przepustowości przez program DPM i usługi IIS przekraczają limit przepustowości zasad grupy, więc w rezultacie limit programu DPM może nie zostać zastosowany. Aby rozwiązać ten problem, zmniejsz ustawienie programu DPM określające ograniczanie przepustowości sieci.

Włączanie kompresji danych

Kompresja w locie jest konfigurowana na poziomie grupy ochrony dla kopii zapasowych na taśmie. Kompresja danych zmniejsza ilość miejsca wymaganego na taśmach i zwiększa liczbę zadań tworzenia kopii zapasowej, które

można przechowywać na tej samej taśmie. Kompresja nie zwiększa w znacznym stopniu czasu wymaganego do ukończenia zadania tworzenia kopii zapasowej. Szyfrowanie zwiększa bezpieczeństwo danych i również nie zwiększa w znacznym stopniu czasu wymaganego do ukończenia zadania tworzenia kopii zapasowej. Szyfrowanie wymaga prawidłowego certyfikatu na serwerze programu DPM. Skonfiguruj kompresję w następujący sposób:

1. Otwórz konsolę administratora programu DPM i przejdź do widoku **Ochrona**.
2. Kliknij pozycję **Optymalizuj wydajność**. Na karcie **Sieć** zaznacz opcję **Włącz kompresję podczas transmisji**.

Różnicowanie godzin rozpoczęcia synchronizacji

W celu optymalizacji wydajności można przesunąć godziny rozpoczęcia zadań synchronizacji dla poszczególnych grup ochrony tak, aby nie wszystkie elementy były uruchamiane w tym samym czasie. Przesunięcie godziny rozpoczęcia synchronizacji umożliwia także optymalizację dodatkowej ochrony innego serwera DPM. Dokonaj przesunięcia w następujący sposób:

1. Otwórz konsolę administratora programu DPM i przejdź do widoku Ochrona, a następnie wybierz grupę ochrony.
2. Kliknij pozycję **Optymalizuj wydajność**. Na karcie Sieć wybierz godziny i minuty, aby przesunięto początek zadania synchronizacji w polu **przesunięcia** <czas> godzina rozpoczęcia według.

Optymalizacja tworzenia ekspresowych kopii zapasowych

Aby zapewnić szybkie odzyskiwanie danych aplikacji, program DPM musi okresowo tworzyć ekspresowe pełne kopie zapasowe. Tworzenie ekspresowej pełnej kopii zapasowej zwykle zwiększa na kilka minut zapotrzebowanie na zasoby serwera o 5 procent. Aby zmniejszyć obciążenie zasobów serwera, można zaplanować rzadsze wykonywanie ekspresowych kopii zapasowych przy równoczesnym zwiększeniu czasu odzyskiwania danych. Zmodyfikuj harmonogram w następujący sposób:

1. Otwórz konsolę administratora programu DPM i przejdź do widoku **Ochrona**, a następnie wybierz grupę ochrony, dla której chcesz zmodyfikować harmonogram ekspresowych pełnych kopii zapasowych.
2. Kliknij pozycję **Optymalizuj wydajność** na karcie **Ekspresowa pełna kopia zapasowa**, wybierz dostępne godziny wykonywania ekspresowych pełnych kopii zapasowych i kliknij przycisk **Dodaj**. Wybierz dni tygodnia, w których będą wykonywane ekspresowe pełne kopie zapasowe.

Zarządzanie wieloma serwerami DPM za pomocą programu Central Console

10.01.2020 • 5 minutes to read

Konsola centralna to konsola System Center Operations Manager, którą można wdrożyć w celu zarządzania wieloma serwerami programu System Center Data Protection Manager (DPM) i ich monitorowania z jednej lokalizacji. Umożliwia ona:

- Scentralizowane monitorowanie serwerów programu DPM z jednej lokalizacji — można monitorować różne wersje programu DPM oraz śledzić stan serwerów, zadań, zasobów chronionych, bibliotek taśm, dostępnego magazynu i miejsca na dysku.
- Kontrolę dostępu opartą na rolach.
- Zdalne odzyskiwanie i zdalne akcje naprawcze.
- Wysyłanie alertów na podstawie Umowy dotyczącej poziomu usług (SLA) oraz konsolidowanie alertów — alerty są generowane, gdy umowa SLA zostaje zerwana. Można konsolidować alerty i pracować nad elementami o wysokim priorytecie w następujący sposób:
 - Powtórzone alerty — wyświetlanie tylko jednego alertu dla powtórzonych alertów. Na przykład jeśli zaplanowane zadanie ma być uruchamiane co godzinę i nie zostało uruchomione w ciągu ostatnich 10 godzin, zostanie wyświetlony tylko jeden alert dla zadania zakończonego niepowodzeniem.
 - Taka sama główna przyczyna — jeśli wiele alertów ma taką samą główną przyczynę lub jeśli wiele kopii zapasowych tego samego źródła danych ulega awarii, generowane są tylko alerty informujące o awarii.
 - Generowanie biletów — w przypadku używania systemu obsługi biletów generowany jest tylko jeden bilet.
- Konsola zakresu — jest oparta na konsoli administratora programu DPM (z niewielkimi różnicami).

Konfigurowanie programu Central Console

Program Central Console można zainstalować na serwerze z systemem Windows Server 2008 R2 lub nowszym albo na komputerze klienckim z systemem Windows 7 lub nowszym. Nie można go zainstalować na serwerze programu DPM. Aby go skonfigurować, zainstaluj odpowiedniego agenta programu Operations Manager na każdym serwerze DPM, którym chcesz zarządzać, a następnie zainstaluj program Central Console na serwerze programu Operations Manager przez zaimportowanie pakietu administracyjnego programu DPM, a następnie zainstalowanie konsoli.

1. Wdróż agenta programu Operations Manager na serwerze DPM. [Przeczytaj więcej](#).
2. Program Central Console składa się z dwóch pakietów administracyjnych:
Microsoft.SystemCenter.DataProtectionManager.2012.Discovery.mp i
Microsoft.SystemCenter.DataProtectionManager.2012.Library.mp. Należy zaimportować oba te elementy, które znajdują się w <Napędcd: > \Management Pack. Podczas importowania pakietu administracyjnego system Windows wyświetli ostrzeżenie o akcjach zapisu. Jest to oczekiwane ostrzeżenie. Możesz kliknąć przycisk **OK**, aby kontynuować.

Należy zauważyć, że program Central Console wymaga wersji pakietu administracyjnego, która jest dostępna w folderze instalacji programu DPM. Jednak po zainstalowaniu tej wersji można przeprowadzić

aktualizację do najnowszej wersji pakietu administracyjnego, która jest dostępna w [Centrum pobierania](#).

3. Po zaimportowaniu pakietu zainstaluj program Central Console. Aby to zrobić, na ekranie Instalatora programu Operations Manager wybierz opcję **Zainstaluj składniki serwerowe i klienckie programu Central Console**, jeśli chcesz monitorować serwery DPM, na których znajduje się agent programu Operations Manager i korzystać z konsoli administratora programu DPM. Wybierz opcję **Zainstaluj program Central Console**, jeśli chcesz używać tylko konsoli administratora programu DPM bez monitorowania serwera. Wybierz opcję **Zainstaluj składniki serwerowe programu Central Console**, jeśli chcesz tylko monitorować serwery bez korzystania z konsoli administratora programu DPM.
4. Program DPM dodaje wyjątki zapory dla portu 6075 i tworzy domyślną konfigurację dostępu opartą na rolach.
5. Po zainstalowaniu programu Central Console w konsoli programu Operations Manager jest tworzony folder widoku **System Central 2012 Data Protection Manager**. Większością zadań dla zarządzanych serwerów programu DPM można zarządzać z programu Central Console.