

Tworzenie kopii zapasowej stanu systemu i kompletnego stanu systemu

30.04.2019 • Czas czytania: 15 min • 🔍 🔍 🔍

W tym artykule

[Jak działa tworzenie kopii zapasowej stanu systemu](#)

[Wykonywanie kopii zapasowej BMR](#)

[Wymagania wstępne i ograniczenia](#)

[Przed rozpoczęciem](#)

[Tworzenie kopii zapasowej stanu systemu i kompletnego stanu systemu](#)

[Odzyskiwanie stanu systemu lub odzyskiwanie systemu od zera \(BMR\)](#)

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	Odzyskiwane z kopii zapasowej stanu systemu	BM
<p>Dane pliku</p> <p>Regularne tworzenie kopii zapasowej danych</p> <p>Kopia zapasowa stanu systemu/kompletnego stanu systemu</p>	Utracone dane pliku	T	N	N
<p>Dane pliku</p> <p>Kopia zapasowa programu DPM danych pliku</p> <p>Kopia zapasowa stanu systemu/kompletnego stanu systemu</p>	Utracony/uszkodzony system operacyjny	N	T	T
<p>Dane pliku</p> <p>Kopia zapasowa programu DPM danych pliku</p> <p>Kopia zapasowa stanu systemu/kompletnego stanu systemu</p>	Utracony serwer (nieuszkodzone woluminy danych)	N	N	T

Kopia zapasowa	Problem	Odzyskiwanie z kopii zapasowej programu DPM	Odzyskiwane z kopii zapasowej stanu systemu	BM
<p>Dane pliku</p> <p>Kopia zapasowa programu DPM danych pliku</p> <p>Kopia zapasowa stanu systemu/kompletnego stanu systemu</p>	<p>Utracony serwer (utracone woluminy danych)</p>	<p>T</p>	<p>Nie</p>	<p>Tak (Od BM ktoś nas zwy odz kop zap dan plik</p>
<p>Dane programu SharePoint:</p> <p>Kopia zapasowa programu DPM danych farmy</p> <p>Kopia zapasowa stanu systemu/kompletnego stanu systemu</p>	<p>Utracona witryna, listy, elementy listy. dokumenty</p>	<p>T</p>	<p>N</p>	<p>N</p>
<p>Dane programu SharePoint:</p> <p>Kopia zapasowa programu DPM danych farmy</p> <p>Kopia zapasowa stanu systemu/kompletnego stanu systemu</p>	<p>Uszkodzony lub utracony system operacyjny</p>	<p>N</p>	<p>T</p>	<p>T</p>

Kopia zapasowa	Problem	Odzyskiwanie z kopii zapasowej programu DPM	Odzyskiwane z kopii zapasowej stanu systemu	BM
<p>Dane programu SharePoint:</p> <p>Kopia zapasowa programu DPM danych farmy</p> <p>Kopia zapasowa stanu systemu/kompletnego stanu systemu</p>	<p>Odzyskiwanie po awarii</p>	<p>N</p>	<p>N</p>	<p>N</p>
<p>Funkcja Hyper-V</p> <p>Kopia zapasowa programu DPM hosta lub gościa funkcji Hyper-V</p> <p>Kopia zapasowa stanu systemu/kompletnego stanu systemu hosta</p>	<p>Utracona maszyna wirtualna</p>	<p>T</p>	<p>N</p>	<p>N</p>
<p>Funkcja Hyper-V</p> <p>Kopia zapasowa programu DPM hosta lub gościa funkcji Hyper-V</p> <p>Kopia zapasowa stanu systemu/kompletnego stanu systemu hosta</p>	<p>Uszkodzony lub utracony system operacyjny</p>	<p>N</p>	<p>T</p>	<p>T</p>

Kopia zapasowa	Problem	Odzyskiwanie z kopii zapasowej programu DPM	Odzyskiwane z kopii zapasowej stanu systemu	BM
<p>Funkcja Hyper-V</p> <p>Kopia zapasowa programu DPM hosta lub gościa funkcji Hyper-V</p> <p>Kopia zapasowa stanu systemu/kompletnego stanu systemu hosta</p>	<p>Utracony host funkcji Hyper-V (nieuszkodzone maszyny wirtualne)</p>	N	N	T
<p>Funkcja Hyper-V</p> <p>Kopia zapasowa programu DPM hosta lub gościa funkcji Hyper-V</p> <p>Kopia zapasowa stanu systemu/kompletnego stanu systemu hosta</p>	<p>Utracony host funkcji Hyper-V (utracone maszyny wirtualne)</p>	N	N	T
				Od: BM któ nas zwy odz pro DPM
<p>Program SQL Server/Exchange</p> <p>Kopia zapasowa aplikacji programu DPM</p> <p>Kopia zapasowa stanu systemu/kompletnego stanu systemu</p>	<p>Utracone dane aplikacji</p>	T	N	N

Kopia zapasowa	Problem	Odzyskiwanie z kopii zapasowej programu DPM	Odzyskiwane z kopii zapasowej stanu systemu	BM
Program SQL Server/Exchange Kopia zapasowa aplikacji programu DPM Kopia zapasowa stanu systemu/kompletnego stanu systemu	Uszkodzony lub utracony system operacyjny	N	t	T
Program SQL Server/Exchange Kopia zapasowa aplikacji programu DPM Kopia zapasowa stanu systemu/kompletnego 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 stanu systemu	Utracony serwer (utracone dzienniki transakcji i baz danych)	N	N	T Odz BM któ nas zwy odz pro DPI

Jak działa tworzenie kopii zapasowej stanu systemu

1. 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.

2. 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.
3. 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.
4. 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.

- 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 stronie **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 [Deploy the DPM protection agent](#) (Wdrażanie agenta ochrony programu DPM)

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 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 sprawdzenie 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 uruchomienia 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.

Czy ta strona jest pomocna?

 Tak  Nie