

IBM Spectrum Protect for Virtual Environments
Wersja 8.1.6

*Data Protection for VMware —
Podręcznik instalowania*



IBM Spectrum Protect for Virtual Environments
Wersja 8.1.6

*Data Protection for VMware —
Podręcznik instalowania*



Uwaga:

Przed użyciem informacji zamieszczonych w tej publikacji i opisywanych produktów należy przeczytać sekcję “Uwagi” na stronie 125.

Niniejsze wydanie dotyczy wersji 8, wydania 1, modyfikacji 6 programu IBM Spectrum Protect for Virtual Environments (numer produktu 5725-X00) i wszystkich następnych jego wydań i modyfikacji, dopóki nie zostanie to określone inaczej w nowych wydaniach.

© Copyright IBM Corporation 2011, 2018.

Spis treści

Informacje o publikacji v

Dla kogo przeznaczona jest ta publikacja v

Publikacje v

Co nowego w wersji 8.1.6 vii

Rozdział 1. Instalowanie i aktualizowanie programu Data Protection for VMware . . 1

Komponenty instalowalne 1

Interfejs GUI Data Protection for VMware vSphere . . 3

Agent odtwarzania programu IBM Spectrum Protect . . 6

Wtyczka klienta IBM Spectrum Protect vSphere . . 6

Interfejs wiersza komend Data Protection for VMware

Interfejs odtwarzania plików programu IBM Spectrum

Protect 8

Składnik: narzędzie przenoszenia danych 8

Planowanie instalacji programu Data Protection for
VMware. 10

Instalacja - przewodnik przejścia 10

Scenariusze instalacji 11

Wymagania systemowe 12

Instalowanie komponentów programu Data Protection for
VMware. 22

Uzyskiwanie pakietu instalacyjnego programu Data
Protection for VMware 22

Instalowanie komponentów programu Data Protection
for VMware za pomocą kreatora instalacji. 23

Instalowanie komponentów programu Data Protection
for VMware w trybie cichym 27

Pierwsze kroki po zainstalowaniu programu Data
Protection for VMware 29

Aktualizowanie programu Data Protection for VMware. . 31

Aktualizowanie programu Data Protection for VMware

Aktualizowanie programu Data Protection for VMware

w 64-bitowym systemie Windows w trybie cichym . . 32

Aktualizowanie programu Data Protection for VMware

w systemie Linux w trybie cichym 33

Deinstalowanie programu Data Protection for VMware. . 34

Deinstalowanie programu Data Protection for VMware

w systemie Windows 34

Deinstalowanie programu Data Protection for VMware

w systemie Windows w trybie cichym 35

Deinstalowanie programu Data Protection for VMware

w systemie Linux 36

Modyfikowanie istniejącej instalacji produktu Data
Protection for VMware 38

Modyfikowanie pakietów w istniejącej instalacji
produktu Data Protection for VMware 39

Modyfikowanie składników w istniejącej instalacji
produktu Data Protection for VMware 39

Rozdział 2. Konfigurowanie programu Data Protection for VMware 41

Konfigurowanie nowej instalacji za pomocą kreatora . . 41

Używanie notatnika do edytowania istniejącej instalacji . 42

Włączanie w środowisku obsługi odtwarzania plików . 43

Konfigurowanie operacji odtwarzania plików w
systemie Linux. 44

Modyfikowanie opcji na potrzeby operacji odtwarzania
plików 45

Opcje odtwarzania plików 46

Konfigurowanie aktywności dziennika dla operacji
odtworzenia plików 47

Opcje aktywności dziennika odtwarzania plików. . . 48

Konfigurowanie węzła narzędzia przenoszenia danych do
obsługi znaczników 48

Konfigurowanie środowiska dla operacji
natychmiastowego odtwarzania pełnej maszyny wirtualnej. 53

1. Konfigurowanie oprogramowania iSCSI na hoście
ESXi. 53

2. Instalowanie i konfigurowanie aplikacji w narzędziu
przenoszenia danych 54

3. Konfigurowanie połączenia agenta odtwarzania . . 54

4. Konfigurowanie dedykowanej sieci iSCSI dla hosta
ESXi i narzędzia przenoszenia danych. 55

Konfigurowanie ustawień zabezpieczeń dla produktu Data
Protection for VMware 56

Konfigurowanie ustawień zabezpieczeń w celu
połączenia narzędzia przenoszenia danych i węzłów

VMCLI z serwerem IBM Spectrum Protect 57

Konfigurowanie komunikacji interfejsu GUI Data
Protection for VMware vSphere z użyciem protokołu

TLS 62

Wymagania dotyczące uprawnień użytkownika serwera
VMware vCenter 69

Role użytkowników w interfejsie GUI Data Protection for
VMware vSphere 72

Klucze rejestracji interfejsu GUI programu Data Protection
for VMware 75

Konfigurowanie interfejsu GUI programu agent
odtworzenia. 76

Włączanie bezpiecznej komunikacji od komponentu
agent odtwarzania do serwera IBM Spectrum Protect . 81

Ustawienia narodowe 84

Działanie plików dzienników 85

Uruchamianie usług dla produktu Data Protection for
VMware i ich działanie 87

Dodatek A. Zaawansowane czynności konfiguracyjne 89

Konfigurowanie węzłów IBM Spectrum Protect w
środowisku vSphere 90

Konfigurowanie węzłów narzędzia przenoszenia danych w
interfejsie GUI wtyczki vSphere 91

Ręczne konfigurowanie węzłów narzędzia przenoszenia
danych w środowisku vSphere 93

Konfigurowanie interfejsu wiersza komend Data
Protection for VMware w środowisku vSphere 97

Lista kontrolna konfiguracji interfejsu wiersza komend środowiska vSphere	99
Taśmy: wytyczne dotyczące konfigurowania	102
Ręczne konfigurowanie urządzenia iSCSI w systemie Linux	104
Ręczne konfigurowanie urządzenia iSCSI w systemie Windows	107
Ręczne konfigurowanie węzłów proxy podłączania w systemie Linux	109
Ręczne konfigurowanie węzłów proxy podłączania w zdalnym systemie Windows	111
Ręczne konfigurowanie wielu akceptorów klienta w systemie Linux	113
Modyfikowanie pliku konfiguracyjnego interfejsu VMCLI	115

Dodatek B. Migrowanie do strategii kopii zapasowej typu zawsze przyrostowa - przyrostowa.	117
--	------------

Dodatek C. Ułatwienia dostępu w rodzinie produktów IBM Spectrum Protect	123
--	------------

Uwagi.	125
-----------------------	------------

Glosariusz.	129
----------------------------	------------

Indeks	131
-------------------------	------------

Informacje o publikacji

Program IBM Spectrum Protect for Virtual Environments umożliwia tworzenie przyrostowych kopii zapasowych i odtwarzanie plików na poziomie bloków poza hostem, a także natychmiastowe odtwarzanie z pełnych kopii zapasowych maszyn wirtualnych dla maszyn typu gość w systemach Windows i Linux. Przyrostowe kopie zapasowe na poziomie bloków można tworzyć wtedy, gdy program IBM Spectrum Protect for Virtual Environments jest używany z narzędziem przenoszenia danych IBM Spectrum Protect.

Dla kogo przeznaczona jest ta publikacja

Ta publikacja jest przeznaczona dla administratorów i użytkowników, którzy chcą zainstalować i skonfigurować program IBM Spectrum Protect for Virtual Environments.

Przegląd informacji, czynności wykonywane przez użytkownika, scenariusze tworzenia i odtwarzania kopii zapasowych, skorowidz komend i komunikaty o błędach są opisane w publikacji *IBM Spectrum Protect for Virtual Environments: Data Protection for VMware – Podręcznik użytkownika*.

Publikacje

Rodzina produktów IBM Spectrum Protect obejmuje produkty IBM Spectrum Protect Plus, IBM Spectrum Protect for Virtual Environments, IBM Spectrum Protect for Databases i szereg innych produktów do zarządzania pamięcią masową w systemie IBM®.

Aby wyświetlić dokumentację produktów IBM, patrz Centrum Wiedzy IBM.

Co nowego w wersji 8.1.6

W programie IBM Spectrum Protect for Virtual Environments w wersji 8.1.6 wprowadzono nowe funkcje i aktualizacje.

Listę nowych funkcji i aktualizacji w tej i w poprzednich wersjach 8 programu zawiera sekcja Aktualizacje programu Data Protection for VMware.

Nowe i zmienione informacje zamieszczone w tej publikacji zostały oznaczone pionową kreską (!) po lewej stronie.

Rozdział 1. Instalowanie i aktualizowanie programu Data Protection for VMware

Instalacja programu IBM Spectrum Protect for Virtual Environments obejmuje planowanie, instalowanie i początkowe konfigurowanie.

Komponenty instalowalne

Program Data Protection for VMware zawiera szereg komponentów, które można zainstalować w celu ochrony środowiska wirtualnego.

W zależności od środowiska systemu operacyjnego następujące składniki programu Data Protection for VMware są dostępne do zainstalowania:

Ograniczenie: Każdy pakiet instalacyjny przedstawia użytkownikowi plik z licencją użytkownika (EULA). Jeśli ten plik nie zostanie zaakceptowany, instalacja zostanie zatrzymana.

Tabela 1. Dostępne składniki programu Data Protection for VMware wg systemu operacyjnego

Komponent	Linux	Windows
Agent odtwarzania programu IBM Spectrum Protect Ten komponent udostępnia możliwości podłączenia wirtualnego i natychmiastowego odtwarzania.		√
Interfejs wiersza komend agenta odtwarzania Interfejs wiersza komend używany na potrzeby operacji podłączania.		√
Dokumenty Wśród dokumentów znajdują się pliki readme i pliki z uwagami.	√	√
Plik zezwolenia programu Data Protection for VMware Ten komponent umożliwia programowi IBM Spectrum Protect uruchamianie następujących typów kopii zapasowych: <ul style="list-style-type: none">• Kopia zapasowa zawsze przyrostowa - przyrostowa• Kopia zapasowa typu zawsze przyrostowa - pełna Ten komponent jest wymagany do ochrony aplikacji. W przypadku nieobciążającego tworzenia kopii zapasowej ten plik musi być zainstalowany na serwerze kopii zapasowych vStorage.	√	√

Tabela 1. Dostępne składniki programu Data Protection for VMware wg systemu operacyjnego (kontynuacja)

Komponent	Linux	Windows
<p>interfejs GUI Data Protection for VMware vSphere</p> <p>Ten komponent jest graficznym interfejsem użytkownika (GUI), który uzyskuje dostęp do danych maszyny wirtualnej na serwerze VMware vCenter. Zawartość tego interfejsu GUI jest dostępna w następujących widokach:</p> <ul style="list-style-type: none"> • Widok przeglądarki WWW. Ten widok jest dostępny w obsługiwanej przeglądarce WWW za pomocą adresu URL hosta serwera WWW interfejsu GUI. Na przykład: https://guihost.mycompany.com:9081/TsmVMwareUI/ • Widok wtyczka klienta IBM Spectrum Protect vSphere w kliencie VMware vSphere Web Client. Panele w tym widoku są jednoznacznie zaprojektowane w taki sposób, aby zapewnić integrację w kliencie WWW, ale dane i komendy na potrzeby tego widoku są pobierane z tego samego serwera WWW interfejsu GUI, z którego są pobierane dla innych widoków. Komponent wtyczka klienta IBM Spectrum Protect vSphere udostępnia podzbiór funkcji, które są dostępne w widoku przeglądarki WWW, a także pewne dodatkowe funkcje. Konfigurowanie i zaawansowane funkcje raportowania nie są obsługiwane w tym widoku. <p>Podczas instalacji można określić jeden lub więcej widoków.</p>	✓	✓
<p>Interfejs GUI odtwarzania plików</p> <p>Ten komponent jest internetowym interfejsem GUI służącym do odtwarzania plików z kopii zapasowych maszyn wirtualnych VMware bez pomocy administratora. Ten interfejs GUI jest instalowany automatycznie podczas instalowania interfejsu GUI programu Data Protection for VMware. Aktywuje się go za pomocą kreatora konfiguracji.</p>	¹	✓
<p>Narzędzie przenoszenia danych</p> <p>Narzędzie przenoszenia danych należące do programu IBM Spectrum Protect służy do przenoszenia danych na potrzeby programu Data Protection for VMware. Ta funkcja jest zwana narzędziem przenoszenia danych. Narzędzie przenoszenia danych przenosi dane ze środowiska wirtualnego do serwera IBM Spectrum Protect. Po zainstalowaniu narzędzia przenoszenia danych na serwerze można używać tego serwera jako serwera kopii zapasowych vStorage. Narzędzie przenoszenia danych można zainstalować w tym samym systemie co program Data Protection for VMware lub na innym serwerze.</p>	✓	✓

1. Chociaż komponent odtwarzania plików należy zainstalować i aktywować w systemie Windows, tego interfejsu można używać do odtwarzania plików na maszynach wirtualnych typu gość zarówno w systemach Windows, jak i Linux.
2. Klienta kopii zapasowych i archiwalnych i narzędzia przenoszenia danych programu Data Protection for VMware nie można zainstalować w tym samym systemie Windows lub Linux.

Program Data Protection for VMware przenosi obciążenie maszyn wirtualnych związane z tworzeniem kopii zapasowych na serwer kopii zapasowych vStorage. Aby wykonać to

zadanie, na serwerze kopii zapasowych vStorage musi być zainstalowane narzędzie przenoszenia danych w wersji 8.1.4.

Interfejs GUI Data Protection for VMware vSphere

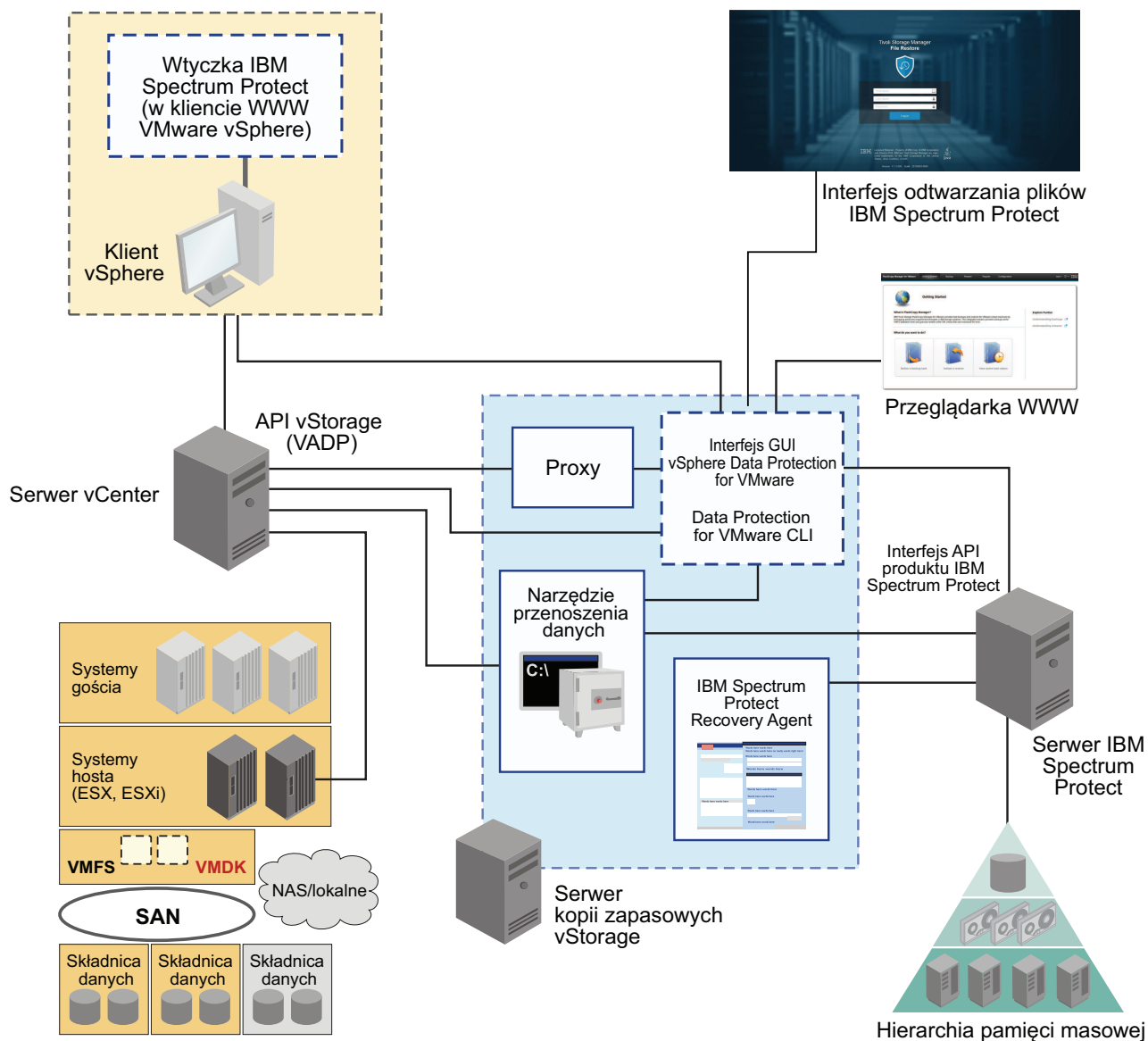
Komponent Interfejs GUI Data Protection for VMware vSphere (interfejs GUI środowiska vSphere) jest graficznym interfejsem użytkownika, który uzyskuje dostęp do danych maszyny wirtualnej na serwerze VMware vCenter.

Przegląd

Interfejs GUI Data Protection for VMware vSphere jest podstawowym interfejsem, w którym można wykonywać następujące czynności:

- Inicjowanie lub planowanie tworzenia kopii zapasowych maszyn wirtualnych na serwerze IBM Spectrum Protect.
- Inicjowanie pełnego odtwarzania maszyn wirtualnych z serwera IBM Spectrum Protect.
- Generowanie raportów o postępie zadań, najnowszych zdarzeniach, które zostały zakończone, statusie tworzenia kopii zapasowych i o użyciu miejsca. Informacje te mogą być pomocne podczas rozwiązywania problemów z kopiami zapasowymi.

Wskazówka: Informacje o tym, w jaki sposób można wykonywać czynności za pomocą interfejsu GUI środowiska vSphere, są dostępne w pomocy elektronicznej instalowanej razem z interfejsem GUI. Kliknięcie opcji **Dowiedz się więcej** w dowolnym oknie interfejsu GUI powoduje otwarcie pomocy elektronicznej zapewniającej asystę do wykonywanych czynności.



Rysunek 1. Komponenty systemu Data Protection for VMware w środowisku użytkownika VMware vSphere

Wymagania

Interfejs GUI Data Protection for VMware vSphere można zainstalować w dowolnym systemie, który spełnia wymagania wstępne dotyczące systemu operacyjnego. Wymagania dotyczące zasobów dla interfejsu GUI środowiska vSphere są minimalne, ponieważ interfejs ten nie przetwarza przesyłania danych we/wy.

Wskazówka: Zainstalowanie interfejsu GUI środowiska vSphere na serwerze kopii zapasowych vStorage jest najczęściej stosowaną konfiguracją.

Interfejs GUI środowiska vSphere musi mieć połączenie sieciowe z następującymi systemami:

- Serwer vStorage Backup Server
- Serwer IBM Spectrum Protect
- Serwer vCenter

Ponadto muszą być dostępne porty dla bazy danych Derby (domyślnie 1527) i serwera WWW interfejsu GUI (domyślnie 9081).

Konfiguracja

Na jednym serwerze vCenter można zarejestrować wiele interfejsów GUI środowiska vSphere. Scenariusz ten ogranicza liczbę centrów przetwarzania danych (i kopii zapasowych ich maszyn wirtualnych typu gość) zarządzanych przez pojedynczy interfejs GUI środowiska VMware vSphere. Serwer vCenter może następnie zarządzać podzbiorem wszystkich centrów przetwarzania danych zdefiniowanych na serwerze vCenter.

Aby zaktualizować zarządzane centra przetwarzania danych, kliknij kolejno opcje **Konfiguracja > Edytuj konfigurację**.

Gdy na jednym serwerze vCenter rejestrowanych jest wiele interfejsów GUI środowiska vSphere, obowiązują następujące wytyczne:

- Każde centrum przetwarzania danych może być zarządzane tylko przez jeden zainstalowany interfejs GUI środowiska vSphere.
- Dla każdego zainstalowanego interfejsu GUI środowiska vSphere wymagana jest unikalna nazwa węzła interfejsu VMCLI.
- Używanie unikalnych nazw węzłów narzędzi przenoszenia danych dla każdego zainstalowanego interfejsu GUI środowiska vSphere upraszcza zarządzanie węzłami.

Uzyskiwanie dostępu do interfejsu GUI środowiska vSphere

Dostęp do interfejsu GUI środowiska vSphere można uzyskać za pomocą następujących metod:

- Autonomiczny interfejs GUI w przeglądarce WWW. Ten interfejs GUI jest dostępny za pomocą zakładki z adresem URL do serwera WWW interfejsu GUI, na przykład:
`https://nazwa_hosta:port/TsmVMwareUI/`
gdzie:
 - *nazwa_hosta* oznacza nazwę systemu, w którym zainstalowano interfejs GUI Data Protection for VMware vSphere
 - *port* oznacza numer portu, na którym interfejs GUI środowiska vSphere jest dostępny. Domyślnym numerem portu jest 9081.
- Rozszerzenie vSphere Web Client, które pozwala serwerowi WWW interfejsu GUI uzyskać dostęp do maszyn wirtualnych w pamięci masowej IBM (zwane rozszerzeniem ochrony danych). Jego zawartość stanowi podzbiór zawartości dostępnej w interfejsie GUI w przeglądarce WWW.

Podczas instalacji można określić jedną lub więcej metod dostępu.

Windows Domyślnym katalogiem instalacyjnym jest C:\IBM\SpectrumProtect\webserver.

Linux Domyślnym katalogiem instalacyjnym jest /opt/tivoli/tsm/tdpvmware/common/webserver.

Agent odtwarzania programu IBM Spectrum Protect

Usługa agenta odtwarzania umożliwia podłączenie dowolnego woluminu obrazu stanu z serwera IBM Spectrum Protect.

Przegląd

Aby uzyskać zdalny dostęp do obrazu stanu, można użyć protokołu iSCSI.

Aby przejrzeć obraz stanu lokalnie w systemie klienta w trybie tylko do odczytu, należy użyć programu Data Protection for VMware w wersji 8.1.4 lub wcześniejszej.

Dodatkowo agent odtwarzania udostępnia funkcję natychmiastowego odtwarzania i ochrony aplikacji w systemie typu gość. Natychmiastowe odtwarzanie umożliwia zachowanie dostępności używanego woluminu, gdy w tle wykonywana jest operacja odtwarzania. Ochrona aplikacji umożliwia zapewnienie dostępności aplikacji, które zostały zainstalowane w maszynie wirtualnej typu gość, takiej jak Microsoft Exchange Server i Microsoft SQL Server, na potrzeby ochrony operacji tworzenia i odtwarzania kopii zapasowych.

Agent odtwarzania może wykonywać następujące zadania z systemu zdalnego:

- Gromadzenie informacji o danych, które można odtwarzać, na przykład:
 - Kopie zapasowe maszyn wirtualnych.
 - Obrazy stanu dostępne dla kopii zapasowej maszyny wirtualnej.
 - Partycje dostępne w konkretnym obrazie stanu.

Szczegółowe informacje dotyczące komend, parametrów i kodów powrotu zawiera sekcja skorowidzu komend w publikacji *IBM Spectrum Protect for Virtual Environments: Data Protection for VMware: Podręcznik użytkownika*.

Wymagania

Windows W systemach Windows interfejs GUI i interfejs wiersza komend agenta odtwarzania są instalowane podczas pełnej instalacji produktu Data Protection for VMware lub zaawansowanej instalacji narzędzia przenoszenia danych.

Uzyskiwanie dostępu do agenta odtwarzania

Windows Dostęp do agenta odtwarzania można uzyskać z menu **Start**: **Start > IBM Spectrum Protect > IBM Spectrum Protect for Virtual Environments > Agent odtwarzania programu IBM Spectrum Protect**.

Wtyczka klienta IBM Spectrum Protect vSphere

Komponent wtyczki klienta IBM Spectrum Protect vSphere jest rozszerzeniem środowiska VMware vSphere Web Client, które udostępnia widok interfejsu GUI programu Data Protection for VMware vSphere.

Przegląd

Komponent wtyczki klienta IBM Spectrum Protect vSphere udostępnia podzbiór funkcji, które są dostępne w widoku przeglądarki dla interfejsu GUI programu Data Protection for VMware vSphere, a także pewne dodatkowe funkcje.

Wymaganie

Aby zainstalować komponent wtyczka klienta IBM Spectrum Protect vSphere, należy wybrać następujące opcje po uruchomieniu kreatora konfiguracji programu IBM Spectrum Protect for Virtual Environments:

- Na stronie **Ustawienia vCenter** kreatora konfiguracji wybierz opcję **Rejestracja aktualizacji**, aby zarejestrować wtyczkę na powiązanym serwerze vCenter.
- Podaj adres hosta interfejsu GUI, użytkownika i hasło serwera vCenter.

Po zakończeniu pracy kreatora wtyczka zostanie zarejestrowana na serwerze vCenter.

Uzyskiwanie dostępu do rozszerzenia ochrony danych

Dostęp do rozszerzenia można uzyskać z poziomu klienta WWW vSphere.

Interfejs wiersza komend Data Protection for VMware

Interfejs CLI Data Protection for VMware jest w pełni funkcjonalnym interfejsem wiersza komend instalowanym z interfejsem GUI Data Protection for VMware vSphere.

Przegląd

Za pomocą interfejsu CLI Data Protection for VMware można wykonywać następujące czynności:

- Inicjowanie lub planowanie tworzenia kopii zapasowych maszyn wirtualnych na serwerze IBM Spectrum Protect.
- Inicjowanie pełnego odtwarzania maszyn wirtualnych, plików maszyn wirtualnych lub dysków maszyn wirtualnych (VMDK) z serwera IBM Spectrum Protect.
- Wyświetlanie informacji konfiguracyjnych dotyczących bazy danych kopii zapasowych i środowiska.

Chociaż interfejs GUI Data Protection for VMware vSphere jest podstawowym interfejsem do wykonywania zadań, interfejs CLI Data Protection for VMware udostępnia przydatny interfejs dodatkowy.

Na przykład interfejsu CLI Data Protection for VMware można użyć do zaimplementowania mechanizmu planowania innego niż mechanizm implementowany przez interfejs GUI Data Protection for VMware vSphere. Ponadto interfejs CLI Data Protection for VMware jest przydatny w przypadku oceniania wyników automatyzacji za pomocą skryptów.

Uzyskiwanie dostępu do interfejsu wiersza komend Data Protection for VMware

Dostęp do interfejsu CLI Data Protection for VMware można uzyskać za pomocą wiersza komend.

Szczegółowe informacje dotyczące dostępnych komend zawiera sekcja skorowidzu komend w publikacji *IBM Spectrum Protect for Virtual Environments: Data Protection for VMware: Podręcznik użytkownika*.

Interfejs odtwarzania plików programu IBM Spectrum Protect

Istnieje możliwość odtwarzania pojedynczych plików z kopii zapasowej maszyny wirtualnej VMware.

Przegląd

Interfejs odtwarzania plików jest interfejsem WWW umożliwiającym odtwarzanie pojedynczych plików z kopii zapasowych maszyn wirtualnych. Zaletą tego interfejsu jest to, że właściciele plików, oprogramowania i platform mogą odtwarzać swoje pliki bez wiedzy na temat operacji tworzenia i odtwarzania kopii zapasowych w programie IBM Spectrum Protect.

Składnik w postaci interfejsu do odtwarzania plików jest instalowany po wybraniu opcji ochrony danych w środowisku vSphere. W kreatorze konfiguracji programu Data Protection for VMware należy aktywować składnik odtwarzania plików dla interfejsu, którym ma być dostępny.

Uzyskiwanie dostępu do interfejsu do odtwarzania plików w programie IBM Spectrum Protect

Aby uzyskać dostęp do interfejsu odtwarzania plików, otwórz przeglądarkę WWW i wprowadź adres URL podany przez administratora. Na przykład:

`https://nazwa_hosta:9081/FileRestoreUI`

gdzie *nazwa_hosta* oznacza nazwę systemu, w którym zainstalowano interfejs GUI Data Protection for VMware vSphere.

Składnik: narzędzie przenoszenia danych

Narzędzie przenoszenia danych jest komponentem oprogramowania Data Protection for VMware, który służy do przenoszenia danych do i z serwera IBM Spectrum Protect.

Przegląd

W typowym środowisku VMware narzędzie przenoszenia danych jest używane do zapisywania kopii zapasowych maszyn wirtualnych do węzła centrum przetwarzania danych.

Gdy instalowany jest produkt Data Protection for VMware, instalacja ta obejmuje narzędzie przenoszenia danych. Narzędzie przenoszenia danych jest instalowane w tym samym systemie co interfejs GUI programu Data Protection for VMware vSphere i inne komponenty produktu Data Protection for VMware.

Narzędzia przenoszenia danych można także instalować w systemach zdalnych, niezależnie od innych komponentów produktu Data Protection for VMware, aby rozłożyć obciążenie związane z tworzeniem kopii zapasowych na wiele systemów.

Operacje tworzenia różnicowej kopii zapasowej obrazu stanu nie są obsługiwane w środowisku VMware. Nie można uruchomić operacji tworzenia różnicowej kopii zapasowej obrazu stanu systemu plików, który znajduje się w zarządcy plików NetApp na gościu, na którym zainstalowano również narzędzie przenoszenia danych programu Data Protection for VMware.

Konfigurowanie narzędzi przenoszenia danych

Aby uzyskać informacje na temat planowania, instalowania i konfigurowania narzędzi przenoszenia danych, przejrzyj poniższą listę:

Działanie	Opis
Określ liczbę narzędzi przenoszenia danych, które są wymagane do ochrony środowiska vSphere.	<p>Do ochrony środowiska vSphere może być wymaganych wiele węzłów narzędzia przenoszenia danych.</p> <p>Aby określić liczbę wymaganych węzłów narzędzia przenoszenia danych, patrz nota techniczna 2007197. Ta nota techniczna zawiera również uwagi dotyczące używania maszyn wirtualnych i komputerów fizycznych dla węzłów narzędzia przenoszenia danych, a także położenia narzędzia przenoszenia danych.</p>
Zainstaluj produkt Data Protection for VMware.	<p>Aby zainstalować produkt Data Protection for VMware, uruchom instalator produktu Data Protection for VMware i wybierz opcję Instalacja typowa dla systemów operacyjnych Windows lub opcję Kompletna dla systemów operacyjnych Linux. Ta opcja instalacji spowoduje zainstalowanie wszystkich komponentów produktu Data Protection for VMware, w tym narzędzia przenoszenia danych.</p> <p>Informacje na temat uruchamiania instalatora produktu Data Protection for VMware zawiera sekcja “Instalowanie komponentów programu Data Protection for VMware” na stronie 22.</p>
Zdefiniuj narzędzia przenoszenia danych dla używanego środowiska.	<p>Gdy kreator instalacji produktu Data Protection for VMware zakończy działanie, zostanie otwarty kreator konfiguracji interfejsu GUI programu Data Protection for VMware vSphere, aby umożliwić użytkownikowi skonfigurowanie komunikacji z serwerem IBM Spectrum Protect.</p> <p>Na stronie Węzły narzędzia przenoszenia danych tego kreatora konfiguracji należy zdefiniować informacje dla lokalnego narzędzia przenoszenia danych i dla wszystkich zdalnych narzędzi przenoszenia danych, które zostaną zainstalowane w oddzielnych systemach.</p> <p>W przypadku instalacji systemie operacyjnym Windows i wybrania opcji Utwórz usługi podczas definiowania narzędzia przenoszenia danych, informacje konfiguracyjne narzędzia przenoszenia danych są zapisywane w pliku opcji w następującym miejscu:</p> <p>C:\Program Files\Tivoli\TSM\baclient\</p> <p>Ponadto konfigurowane są usługi wymagane przez narzędzie przenoszenia danych.</p> <p>Jeśli narzędzie przenoszenia danych jest instalowane w systemie operacyjnym Linux — lub w systemie operacyjnym Windows, ale bez wybierania opcji Utwórz usługi podczas konfigurowania, należy wykonać kroki podane w sekcji “Konfigurowanie węzłów narzędzia przenoszenia danych w interfejsie GUI wtyczki vSphere” na stronie 91, aby utworzyć plik opcji i skonfigurować wymagane usługi.</p>

Działanie	Opis
Zainstaluj i skonfiguruj dodatkowe narzędzia przenoszenia danych w systemach zdalnych, jeśli jest to wymagane.	<p>Aby zainstalować narzędzie przenoszenia danych w systemie zdalnym, uruchom instalator produktu Data Protection for VMware i wykonaj jedną z następujących czynności:</p> <p>W systemach operacyjnych Windows wybierz opcję Instalacja zaawansowana > Zainstaluj tylko narzędzie przenoszenia danych w kreatorze konfiguracji.</p> <p>W systemach operacyjnych Linux wybierz opcję Niestandardowe z listy Zestaw instalacyjny w kreatorze konfiguracji. Upewnij się, że zaznaczona jest opcja Data Protection for VMware — narzędzie przenoszenia danych. Ta opcja jest domyślnie zaznaczona.</p> <p>Po zakończeniu instalacji postępuj zgodnie z instrukcjami zawartymi w sekcji “Konfigurowanie węzłów narzędzia przenoszenia danych w interfejsie GUI wtyczki vSphere” na stronie 91, aby skonfigurować narzędzia przenoszenia danych w systemach zdalnych.</p>

Planowanie instalacji programu Data Protection for VMware

Program Data Protection for VMware eliminuje wpływ tworzenia kopii zapasowych na maszynie wirtualnej, przenosząc obciążenia związane z tworzeniem kopii zapasowej z produktu VMware ESX lub hosta opartego na systemie ESXi na serwer kopii zapasowych vStorage.

Program Data Protection for VMware współpracuje ze zintegrowanym narzędziem przenoszenia danych, aby tworzyć pełne zawsze przyrostowe i przyrostowe zawsze przyrostowe kopie zapasowe maszyn wirtualnych. Węzeł narzędzia przenoszenia danych „przenosi” dane do serwera IBM Spectrum Protect w celu ich przechowywania, a w późniejszym terminie na potrzeby odtwarzania maszyn wirtualnych na poziomie obrazu. Natychmiastowe odtwarzanie jest dostępne na poziomie woluminu dyskowego i pełnej maszyny wirtualnej.

Wskazówka: Narzędzie przenoszenia danych jest oddzielnie licencjonowanym komponentem, który zawiera swoje interfejsy użytkownika i dokumentację. Znajomość tego produktu i jego dokumentacji jest niezbędna, aby poprawnie zintegrować wszechstronny plan ochrony maszyn wirtualnych za pomocą programu Data Protection for VMware. Program Data Protection for VMware dla 64-bitowych systemów Windows zawiera narzędzie przenoszenia danych.

Instalacja - przewodnik przejścia

W poniższej tabeli przedstawiono kroki, które należy wykonać, aby pomyślnie przeprowadzić proces instalowania.

Tabela 2. Czynności instalacyjne dla nowych i istniejących klientów programu Data Protection for VMware

Krok	Zadanie	Zacznij tutaj
1	Sprawdź wymagania systemowe.	Upewnij się, że system, w którym ma zostać zainstalowany program Data Protection for VMware, spełnia wymagania systemowe.

Tabela 2. Czynności instalacyjne dla nowych i istniejących klientów programu Data Protection for VMware (kontynuacja)

Krok	Zadanie	Zaczynij tutaj
2	Sprawdź wymagania dotyczące uprawnień użytkowników.	Uniknij potencjalnych błędów i opóźnień instalacji, stosując wymagane poziomy uprawnień użytkowników.
3	Sprawdź dostępność wymaganych portów komunikacyjnych.	Zapobiegij niepowodzeniom i opóźnieniom instalacji, otwierając wymagane porty komunikacyjne przed przystąpieniem do instalacji programu Data Protection for VMware.
4	<p>Zainstaluj program Data Protection for VMware:</p> <ul style="list-style-type: none"> • Instalowanie programu Data Protection for VMware za pomocą kreatora instalacji • “Instalowanie komponentów programu Data Protection for VMware w trybie cichym” na stronie 27 <p>Zaktualizuj program Data Protection for VMware:</p> <p>Aktualizacja programu Data Protection for VMware</p>	Każdy pakiet instalacyjny przedstawia użytkownikowi plik z licencją użytkownika (EULA). Jeśli ten plik nie zostanie zaakceptowany, instalacja zostanie zakończona.
5	<p>“Konfigurowanie nowej instalacji za pomocą kreatora” na stronie 41</p> <p>Jeśli planowana jest aktualizacja programu Data Protection for VMware, w zależności od tego, które składniki są zainstalowane, może być konieczne wykonanie dodatkowych czynności konfiguracyjnych. Więcej szczegółów zawierają tematy dotyczące konfigurowania w publikacji <i>IBM Spectrum Protect for Virtual Environments: Data Protection for VMware: Podręcznik użytkownika</i>.</p>	Do konfiguracji początkowej użyj kreatora konfiguracji. W zależności od tego, które składniki są zainstalowane, może być konieczne wykonanie dodatkowych czynności konfiguracyjnych, jak to opisano w tej sekcji.

Wskazówka: Aby ułatwić planowanie liczby hostów proxy, które są wymagane dla konkretnego środowiska tworzenia kopii za pomocą programu Data Protection for VMware, w wiki programu IBM Spectrum Protect udostępniono następującą publikację: *Step by Step Guide To vStorage Backup Server (Proxy) Sizing*. Ta publikacja jest dostępna w sekcji dotyczącej produktu IBM Spectrum Protect for Virtual Environments.

Scenariusze instalacji

Przed zainstalowaniem programu Data Protection for VMware należy wybrać scenariusz, który najlepiej spełnia potrzeby biznesowe.

Program Data Protection for VMware i narzędzie przenoszenia danych można zainstalować za pomocą interfejsu GUI lub w trybie cichym:

- “Instalowanie komponentów programu Data Protection for VMware za pomocą kreatora instalacji” na stronie 23
- “Instalowanie komponentów programu Data Protection for VMware w trybie cichym” na stronie 27

Posortowana według platformy lista dostępnych składników i komponentów znajduje się w sekcji “Komponenty instalowalne” na stronie 1.

Tabela 3. Scenariusze instalacji

Numer scenariusza	Opis	Czynności, które należy wykonać
1	Ten scenariusz jest przydatny dla nowej instalacji, w której planowane jest zainstalowanie programu Data Protection for VMware i narzędzia przenoszenia danych w tym samym systemie.	Windows Istnieje możliwość użycia programu Suite Installer w trybie interfejsu GUI lub w trybie cichym. Linux Istnieje możliwość użycia programu InstallAnywhere w trybie interfejsu GUI lub w trybie cichym.
2	Za pomocą tego scenariusza można zainstalować w tym systemie narzędzie przenoszenia danych (proxy podłączania), agenta odtwarzania i wymagane pakiety obsługi.	Windows Istnieje możliwość przeprowadzenia instalacji zaawansowanej za pomocą programu Suite Installer. Linux Składnik narzędzie przenoszenia danych jest obecnie instalowany z programem Data Protection for VMware.

Wymagania systemowe

Aby zaimplementować komponenty programu Data Protection for VMware, system musi spełniać odpowiednie wymagania systemowe.

Wymagania programowe

Szczegóły dotyczące wymagań programowych i wymagań co do systemu operacyjnego mogą się zmieniać. Informacje na temat bieżących wymagań programowych zawiera nota techniczna 1505139.

Wymagania sprzętowe

Wymagania sprzętowe mogą być różne i zależą od następujących elementów:

- Liczba chronionych serwerów
- Liczba chronionych woluminów
- Wielkości zestawów danych
- Połączenia LAN i SAN

Uwaga: Komponent agent odtwarzania nie obsługuje operacji w środowisku bez obciążania sieci LAN.

W poniższej tabeli znajduje się opis wymagań sprzętowych potrzebnych do zainstalowania produktu Data Protection for VMware.

Tabela 4. Wymagania sprzętowe produktu Data Protection for VMware

Komponent	Wymagania minimalne	Preferowane
System	Dwurdzeniowy procesor IntelPentium D 3 GHz lub kompatybilny.	Nie dotyczy

Tabela 4. Wymagania sprzętowe produktu Data Protection for VMware (kontynuacja)

Komponent	Wymagania minimalne	Preferowane
Pamięć	2 GB RAM, 2 GB wirtualnej przestrzeni adresowej.	Nie dotyczy
Dostępny dysk twardy	200 MB na folder 'Documents and Settings'.	2 GB.
Karta NIC	1 NIC - 100 Mb/s.	1 NIC - 1 Gb/s.

Uwaga: W zależności od liczby równolegle przetwarzanych procesów operacje tworzenia kopii zapasowych maszyn wirtualnych wymagają znacznych ilości pamięci.

Wymagania dotyczące pamięci można rozszerzyć dla komendy **dsmc backup vm** i obliczyć za pomocą następującego wzoru:

Wymagana pamięć = (wielkość_dysku / wielkość_MBLK) * wielkość_buforu_odczytu * VM_MAXPARALLEL

gdzie:

- **wielkość_dysku** oznacza wielkość dysku gościa, który obecnie jest przetwarzany;
- **wielkość_MBLK** oznacza wielkość megabloku. Jest to 128 MB dla dysków mniejszych niż 2 TB i 1 GB dla dysków większych niż 2 TB;
- **wielkość_buforu_odczytu** oznacza wielkość wewnętrznego buforu produktu IBM Spectrum Protect, który jest używany do obsługi informacji MBLK. Wielkość tego buforu wynosi 256 kB;
- **VM_MAXPARALLEL** oznacza maksymalną liczbę maszyn wirtualnych, dla których jednocześnie można tworzyć kopie zapasowe w ramach jednego procesu operacji tworzenia kopii zapasowej.

Aby na przykład utworzyć kopię zapasową 10 gości, z których każdy ma dyski o wielkości 40 GB i z parametrem VM_MAXPARALLEL o wartości 2, w ramach jednego procesu operacji tworzenia kopii zapasowej wymagane jest:

- **wielkość_dysku** = 40 GB = 41 943 040 kB;
- **wielkość_MBLK** = 128 MB = 131 072 kB;
- **wielkość_buforu_odczytu** = 256 kB;
- **VM_MAXPARALLEL** = 2.

Wymagana pamięć = (41943040 / 131072) * 256 kB * 2 = 163840 kB = 160 MB.

Uwaga: Aby utworzyć kopie zapasowe takiej samej liczby gości z ustawieniem 'VM_MAXPARALLEL 2' w pięciu równoległych procesach operacji tworzenia kopii zapasowej, wymagane jest (maksymalnie) pięć razy więcej pamięci niż w poprzednim przykładzie (800 MB).

Host proxy Windows jest wymagany dla agenta odtwarzania w systemie Linux. Ten host proxy Windows musi mieć zainstalowanego agenta odtwarzania.

Ograniczenie: Następujące ograniczenia dotyczą dysków VMware VMDK uczestniczących w operacji tworzenia kopii zapasowych:

- W trybie zawsze przyrostowej – przyrostowej kopii zapasowej każdy pojedynczy dysk VMDK uczestniczący w operacji tworzenia kopii zapasowej nie może mieć wielkości przekraczającej 8 TB. Jeśli wielkość dysku VMDK przekroczy 8 TB, operacja tworzenia kopii zapasowej zakończy się niepowodzeniem. Aby zwiększyć wielkość dysku VMDK na

wartość większą niż domyślna wynosząca 2 TB, należy podać wielkość maksymalną za pomocą opcji `vmmaxvirtualdisks`. Więcej informacji na ten temat można znaleźć, wyszukując frazę `vmmaxvirtualdisks` w Centrum Wiedzy IBM.

- W trybie zawsze przyrostowej – pełnej kopii zapasowej każdy pojedynczy dysk VMDK uczestniczący w operacji tworzenia kopii zapasowej nie może mieć wielkości przekraczającej 2 TB. Jeśli wielkość dysku VMDK przekroczy 2 TB, operacja tworzenia kopii zapasowej zakończy się niepowodzeniem.

Aby zapobiec niepowodzeniu w dowolnym z tych trybów tworzenia kopii zapasowej, można pominąć przetwarzanie dysku VMDK przez umieszczenie ustawienia `vmskipmaxvirtualdisks yes` w pliku opcji narzędzia przenoszenia danych. Więcej informacji na ten temat znajduje się w sekcji `Vmskipmaxvirtualdisks`.

Wymagania wstępne dotyczące odtwarzania plików

Zanim rozpocznie się odtwarzanie plików za pomocą interfejsu odtwarzania plików programu IBM Spectrum Protect, należy się upewnić, że używane środowisko spełnia wymagania minimalne.

Aby włączyć opcję odtwarzania plików, program Data Protection for VMware musi być zainstalowany w systemie Windows.

Wymagania wstępne dotyczące maszyny wirtualnej VMware

Następujące wymagania wstępne dotyczą maszyny wirtualnej VMware zawierającej pliki do odtworzenia:

- **Linux** **Windows** Narzędzia VMware Tools muszą być zainstalowane na maszynie wirtualnej.
- **Linux** **Windows** Maszyna wirtualna musi być uruchomiona podczas operacji odtwarzania plików.
- **Windows** Maszyna wirtualna musi należeć do tej samej domeny systemu Windows co system narzędzia przenoszenia danych.
- **Windows** Jeśli maszyna wirtualna zostanie usunięta z domeny systemu Windows, a następnie odtworzona w późniejszym czasie, musi ona z powrotem dołączyć do tej domeny, aby została odtworzona relacja zaufania domen. Nie należy podejmować próby odtwarzania plików z maszyny wirtualnej do momentu, aż zostanie odtworzona relacja zaufania domen.
- **Windows** Jeśli użytkownik nie jest właścicielem pliku, który ma zostać odtworzony, uprawnienie **Przywracaj pliki i katalogi** w systemie Microsoft Windows musi być przypisane do użytkownika dla tej maszyny wirtualnej.
- **Linux** Dla maszyny wirtualnej wymagane jest uwierzytelnianie użytkownika lokalnego. Uwierzytelnianie nie jest dostępne za pomocą domeny systemu Windows, protokołu LDAP (Lightweight Directory Access Protocol), protokołu Kerberos, ani innych metod uwierzytelniania w sieci.
- **Linux** W systemie operacyjnym Red Hat Enterprise Linux 6 opcja `ChallengeResponseAuthentication` w pliku konfiguracyjnym demona `sshd` (`/etc/ssh/sshd_config`) musi mieć wartość `YES` lub musi być przekształcona w komentarz. Na przykład następujące instrukcje są poprawne:
`ChallengeResponseAuthentication yes`
`#ChallengeResponseAuthentication no`

Po zmodyfikowaniu tej opcji zrestartuj demona `sshd`.

Wymagania wstępne dotyczące narzędzia przenoszenia danych

System narzędzia przenoszenia danych reprezentuje szczególne narzędzie przenoszenia danych, które „przenosi dane” z jednego systemu do innego.

Windows System narzędzia przenoszenia danych musi należeć do tej samej domeny systemu Windows co maszyna wirtualna, która zawiera pliki do odtworzenia.

Wymagania wstępne dotyczące proxy podłączania

System proxy podłączania reprezentuje system proxy Linux lub Windows, który uzyskuje dostęp do podłączonych dysków maszyny wirtualnej za pomocą połączenia iSCSI. Ten system umożliwia dostęp do systemów plików na podłączonych dyskach maszyny wirtualnej jako punktów odtwarzania do interfejsu odtwarzania plików.

Linux Systemy operacyjne Linux udostępniają demona, który aktywuje grupy woluminów menedżera woluminów logicznych (LVM), gdy grupy te stają się dostępne dla systemu. Należy ustawić tego demona w systemie proxy podłączania Linux, aby grupy woluminów menedżera woluminów logicznych nie były aktywowane, gdy stają się dostępne dla systemu. Szczegółowe informacje dotyczące sposobu ustawiania tego demona zawiera odpowiednia dokumentacja systemu Linux.

Linux **Windows** System proxy podłączania w systemie Windows i system proxy podłączania w systemie Linux muszą znajdować się w tej samej podsieci.

Wymagania wstępne dotyczące konta domeny systemu Microsoft Windows

Następujące wymagania wstępne dotyczą kont domeny systemu Windows:

- Windows** W celu uzyskania dostępu do sieciowego zasobu współużytkowanego wymagane są informacje autoryzacyjne administratora domeny systemu Windows. Administrator wprowadza te informacje autoryzacyjne w notatniku lub kreatorze konfiguracji interfejsu GUI Data Protection for VMware vSphere w celu aktywowania środowiska na potrzeby operacji odtwarzania plików.
- Windows** Właściciel plików uzyskuje dostęp do zdalnej maszyny wirtualnej, która zawiera pliki do odtworzenia, za pomocą informacji autoryzacyjnych użytkownika domeny systemu Windows. Te informacje autoryzacyjne wprowadza się w interfejsie odtwarzania plików podczas logowania. Informacje autoryzacyjne użytkownika domeny służą do potwierdzenia, że właściciel plików ma uprawnienia do logowania się w zdalnej maszynie wirtualnej i odtwarzania plików do tej zdalnej maszyny wirtualnej. Te informacje autoryzacyjne nie wymagają żadnych uprawnień specjalnych.
- Windows** Jeśli właściciel plików używa konta użytkownika domeny systemu Windows, które ogranicza dostęp do konkretnych komputerów (zamiast ograniczać dostęp do wszystkich komputerów w domenie), należy się upewnić, że system proxy podłączania znajduje się na liście komputerów dostępnych dla tego konta użytkownika domeny. W przeciwnym razie właściciel plików nie będzie mógł zalogować się do interfejsu odtwarzania plików.

Wymagania wstępne dotyczące taśm

Odtwarzanie plików z taśm nie jest obsługiwane. Preferowaną metodą jest odtwarzanie plików z dyskowej pamięci masowej.

Uprawnienia wymagane do instalacji

Przed rozpoczęciem instalacji należy upewnić się, że ID użytkownika ma wymagany poziom uprawnień.

O tym zadaniu

Tabela 5. Uprawnienia użytkowników wymagane do zainstalowania i skonfigurowania programu Data Protection for VMware

System	Wymagane uprawnienie
Windows	Administrator
Linux	Root
Serwer vCenter	Uprawnienia administratora Rola serwera vCenter wymaga następujących uprawnień: Rozszerzenie > rejestrowanie rozszerzenia, wyrejestrowanie rozszerzenia, aktualizowanie rozszerzenia . Ta nowa rola musi zostać zastosowana do obiektu vCenter w hierarchii serwera VMware vCenter dla ID użytkownika określonego podczas instalacji.
Serwer IBM Spectrum Protect Ograniczenie: Serwer musi być uruchomiony.	Dostęp administracyjny (uprawnienie System lub Nieograniczone uprawnienia do domeny)

Wymagane porty komunikacyjne

Lista portów komunikacyjnych, które muszą być otwarte w firewallu podczas instalowania programu Data Protection for VMware.

Porty, które zostały określone w tabeli, odzwierciedlają instalację typową. Instalacja typowa obejmuje następujące komponenty w tym samym systemie Windows:

- Serwer interfejsu GUI programu Data Protection for VMware
- Serwer kopii zapasowych vStorage (narzędzie przenoszenia danych)
- Proxy podłączania Windows
- Interfejs odtwarzania plików programu IBM Spectrum Protect

Jeśli używana jest instalacja inna niż typowa, mogą być wymagane dodatkowe porty.

Ograniczenie: Proxy podłączania Windows i proxy podłączania Linux muszą znajdować się w tej samej podsieci.

Tabela 6. Wymagane porty komunikacyjne. Ta tabela zawiera listę portów, które są używane przez program Data Protection for VMware.

Port TCP	Inicjator: wychodzące (z hosta)	Cel: przychodzące (do hosta)
443	Serwer vStorage Backup Server	Serwer vCenter (bezpieczne połączenie HTTP)
443	Serwer interfejsu GUI Data Protection for VMware vSphere	Serwer vCenter

Tabela 6. Wymagane porty komunikacyjne (kontynuacja). Ta tabela zawiera listę portów, które są używane przez program Data Protection for VMware.

Port TCP	Inicjator: wychodzące (z hosta)	Cel: przychodzące (do hosta)
443 Ustawienie to jest wymagane tylko wtedy, gdy narzędzie przenoszenia danych jest w systemie Linux.	Proxy podłączania Windows	Serwer vCenter
443	Serwer vStorage Backup Server	Platform Services Controller
443	Serwer interfejsu GUI Data Protection for VMware vSphere	Platform Services Controller
443	Proxy podłączania Windows	Platform Services Controller
902 443	Serwer vCenter	Hosty ESXi
902 443	Serwer kopii zapasowych vStorage (proxy)	Hosty ESXi (wszystkie chronione hosty)
1500 (tcpport)	Serwer kopii zapasowych vStorage (proxy)	Serwer IBM Spectrum Protect
1500 (tcpadminport)	<p>Serwer interfejsu GUI Data Protection for VMware vSphere</p> <ul style="list-style-type: none"> 1500 (tcpadminport): komunikacja inna niż SSL Na potrzeby komunikacji SSL tcpadminport jest jedynym portem, który obsługuje komunikację SSL z serwerem IBM Spectrum Protect. Poprawny numer portu do używania z protokołem SSL jest zwykle wartością podaną w opcji ssltcpadminport w pliku dsmserve.opt serwera IBM Spectrum Protect. Jeśli jednak w pliku dsmserve.opt podano opcję adminonclient no, poprawny numer portu dla protokołu SSL jest wartością opcji ssltcpadminport. Opcja ssltcpadminport nie ma wartości domyślnej. Oznacza to, że wartość musi być określona przez użytkownika. 	Serwer IBM Spectrum Protect
1527 Wewnętrzna baza danych Derby		
1501 1581 (httpport)	Serwer IBM Spectrum Protect	<p>Serwer vStorage Backup Server</p> <ul style="list-style-type: none"> Program planujący narzędzia przenoszenia danych Klient WWW Demon akceptora klienta

Tabela 6. Wymagane porty komunikacyjne (kontynuacja). Ta tabela zawiera listę portów, które są używane przez program Data Protection for VMware.

Port TCP	Inicjator: wychodzące (z hosta)	Cel: przychodzące (do hosta)
1581 (httpport) 1582, 1583 (webports)	Serwer interfejsu GUI Data Protection for VMware vSphere	Serwer vStorage Backup Server
9081 Serwer WWW interfejsu GUI (protokół HTTPS)	Klient vSphere	Serwer interfejsu GUI Data Protection for VMware vSphere (bezpieczny port HTTPS na potrzeby dostępu do vCenter za pomocą przeglądarki WWW)
22 Domyślny port SSH dla agenta odtwarzania	Agent odtwarzania	Host „podłączania” Windows programu Data Protection for VMware • SSH dla agenta odtwarzania w systemie Linux
3260	Odtwarzanie plików Data Protection for VMware w systemie Linux	Host „podłączania” Windows programu Data Protection for VMware • iSCSI
3260 Domyślny port iSCSI dla agenta odtwarzania	Cel Windows z dyskiem dynamicznym na potrzeby odtwarzania plików	Host „podłączania” Windows programu Data Protection for VMware • iSCSI
5985	Operacje interfejsu GUI odtwarzania plików	Zdalne zarządzanie systemem Windows
135	Proxy podłączania Windows	Maszyna wirtualna VMware zawierająca pliki do odtworzenia za pomocą interfejsu do odtwarzania plików należącego do programu IBM Spectrum Protect

Wymagania dotyczące uprawnień użytkownika serwera VMware vCenter

Do uruchamiania operacji programu Data Protection for VMware wymagane są określone uprawnienia użytkownika serwera VMware vCenter.

Uprawnienia serwera vCenter wymagane do ochrony centrów przetwarzania danych VMware przy użyciu widoku przeglądarki WWW dla interfejsu GUI Data Protection for VMware vSphere

ID użytkownika serwera vCenter, który loguje się do widoku przeglądarki dla interfejsu GUI Data Protection for VMware vSphere,

musi mieć uprawnienia środowiska VMware wystarczające do wyświetlania treści dla centrum przetwarzania danych, które jest zarządzane za pomocą interfejsu GUI.

Na przykład środowisko VMware vSphere zawiera pięć centrów przetwarzania danych. Użytkownik „jenn” ma wystarczające uprawnienia tylko dla dwóch z tych centrów przetwarzania danych. W związku z tym tylko te dwa centra przetwarzania danych, dla

których istnieją wystarczające uprawnienia, są widoczne dla użytkownika “jenn” w widokach. Pozostałe trzy centra przetwarzania danych (dla których użytkownik “jenn” nie ma uprawnień) nie są widoczne dla tego użytkownika.

Serwer VMware vCenter definiuje zestaw uprawnień łącznie jako rolę. Rola jest stosowana do obiektu dla konkretnego użytkownika lub grupy w celu utworzenia uprawnienia. W kliencie WWW VMware vSphere należy utworzyć rolę z zestawem uprawnień. Aby utworzyć rolę serwera vCenter dla operacji tworzenia i odtwarzania kopii zapasowych, należy użyć funkcji **Add a Role** (Dodaj rolę) klienta VMware vSphere.

Aby propagować uprawnienia do wszystkich centrów przetwarzania danych na serwerze vCenter, należy określić serwer vCenter i zaznaczyć pole wyboru **propagate to children** (propaguj do elementów potomnych). W przeciwnym razie można ograniczyć te uprawnienia, jeśli ta rola zostanie przypisana tylko do wymaganych centrów przetwarzania danych z zaznaczonym polem wyboru **propagate to children** (propaguj do elementów potomnych). Wymuszenie dla interfejsu GUI przeglądarki odbywa się na poziomie centrum przetwarzania danych.

W poniższym przykładzie przedstawiono sposób kontroli dostępu do centrów przetwarzania danych dla dwóch grup użytkowników środowiska VMware. Najpierw należy utworzyć rolę zawierającą wszystkie uprawnienia zdefiniowane w nocie technicznej 7047438. Zbiór uprawnień w tym przykładzie jest identyfikowany za pomocą roli o nazwie “TDPVMwareManage”. Grupa 1 wymaga dostępu do zarządzania maszynami wirtualnymi dla centrów przetwarzania danych Primary1_DC i Primary2_DC. Grupa 2 wymaga dostępu do zarządzania maszynami wirtualnymi dla centrów przetwarzania danych Secondary1_DC i Secondary2_DC.

Dla grupy 1 należy przypisać rolę “TDPVMwareManage” do centrów przetwarzania danych Primary1_DC i Primary2_DC. Dla grupy 2 należy przypisać rolę “TDPVMwareManage” do centrów przetwarzania danych Secondary1_DC i Secondary2_DC.

Użytkownicy w każdej grupie użytkowników środowiska VMware mogą używać interfejsu GUI programu Data Protection for VMware do zarządzania maszynami wirtualnymi tylko w odpowiadających im centrach przetwarzania danych.

Wskazówka: Podczas tworzenia roli należy rozważyć dodanie dodatkowych uprawnień do roli, która może być później potrzebna do wykonania innych czynności na obiektach.

Uprawnienia serwera vCenter wymagane do użycia narzędzia przenoszenia danych

Narzędzie przenoszenia danych programu IBM Spectrum Protect, które jest zainstalowane na serwerze kopii zapasowych vStorage (węzeł narzędzia przenoszenia danych), wymaga opcji VMCUser i VMCPw. Opcja VMCUser określa ID użytkownika serwera vCenter lub ESX, który ma wykonywać operacje tworzenia i odtwarzania kopii zapasowych, a także odpytywania. Wymagane uprawnienia, które są przypisane do tego ID użytkownika (VMCUser), zapewniają, że klient może uruchamiać operacje na maszynie wirtualnej i w środowisku VMware. Ten ID użytkownika musi mieć uprawnienia środowiska VMware, które są opisane w powyższej nodzie technicznej.

Aby utworzyć rolę serwera vCenter dla operacji tworzenia i odtwarzania kopii zapasowych, należy użyć funkcji **Add a Role** (Dodaj rolę) klienta VMware vSphere. Podczas dodawania uprawnień dla tego ID użytkownika (VMCUser) należy wybrać opcję **propagate to children** (propaguj do elementów potomnych). Ponadto należy rozważyć dodanie innych uprawnień do tej roli na potrzeby czynności innych niż tworzenie i odtwarzanie kopii zapasowych. Wymuszanie dla opcji VMCUser odbywa się na poziomie obiektu najwyższego poziomu.

Uprawnienia serwera vCenter wymagane do ochrony centrów przetwarzania danych VMware przy użyciu widoku wtyczki klienta IBM Spectrum Protect vSphere dla interfejsu GUI Data Protection for VMware vSphere

Wtyczka klienta IBM Spectrum Protect vSphere wymaga użycia zestawu uprawnień oddzielnych w stosunku do uprawnień wymaganych do zalogowania się do interfejsu GUI.

Podczas instalowania następujące uprawnienia niestandardowe są tworzone dla wtyczki klienta IBM Spectrum Protect vSphere:

- **Centrum przetwarzania danych > IBM Data Protection**
- **Globalne > Skonfiguruj IBM Data Protection**

Uprawnienia niestandardowe, które są wymagane dla wtyczki klienta IBM Spectrum Protect vSphere, są rejestrowane jako oddzielne rozszerzenie. Kluczem rozszerzenia uprawnień jest `com.ibm.tsm.tdpvmware.IBMDataProtection.privileges`.

Te uprawnienia umożliwiają administratorowi VMware włączanie i wyłączanie dostępu do treści wtyczki klienta IBM Spectrum Protect vSphere. Tylko użytkownicy z tymi uprawnieniami niestandardowymi dla wymaganego obiektu środowiska VMware mogą uzyskać dostęp do treści wtyczki klienta IBM Spectrum Protect vSphere. Jeden komponent wtyczki klienta IBM Spectrum Protect vSphere jest zarejestrowany dla każdego serwera vCenter i jest współużytkowany przez wszystkie hosty interfejsu GUI skonfigurowane do obsługi serwera vCenter.

W kliencie WWW środowiska VMware vSphere należy utworzyć rolę dla użytkowników, którzy mogą wykonywać funkcje ochrony danych dla maszyn wirtualnych za pomocą komponentu wtyczki klienta IBM Spectrum Protect vSphere. Dla tej roli, oprócz uprawnień standardowej roli administratora maszyn wirtualnych wymaganej przez klienta WWW, należy określić uprawnienie **Centrum przetwarzania danych > IBM Data Protection**. Dla każdego centrum przetwarzania danych należy przypisać tę rolę każdemu użytkownikowi lub każdej grupie użytkowników, której chcesz nadać uprawnienie użytkownika służące do zarządzania maszynami wirtualnymi.

Dla użytkownika wymagane jest uprawnienie **Globalne > IBM Data Protection** na poziomie serwera vCenter. To uprawnienie umożliwia użytkownikowi zarządzanie połączeniem między serwerem vCenter i serwerem WWW interfejsu GUI programu Data Protection for VMware vSphere, a także edytowanie i czyszczenie tego połączenia. To uprawnienie należy przypisać administratorom, którzy są zaznajomieni z interfejsem GUI programu Data Protection for VMware vSphere chroniącym ich odpowiedni serwer vCenter. Połączeniami komponentu wtyczki klienta IBM Spectrum Protect vSphere można zarządzać na stronie Połączenia rozszerzenia.

W poniższym przykładzie przedstawiono sposób kontroli dostępu do centrów przetwarzania danych dla dwóch grup użytkowników. Grupa 1 wymaga dostępu do zarządzania maszynami wirtualnymi dla centrów przetwarzania danych `NewYork_DC` i `Boston_DC`. Grupa 2 wymaga dostępu do zarządzania maszynami wirtualnymi dla centrów przetwarzania danych `LosAngeles_DC` i `SanFrancisco_DC`.

W kliencie środowiska VMware vSphere utwórz na przykład rolę `IBMDDataProtectManage`, przypisz uprawnienia standardowej roli administratora maszyn wirtualnych, a także uprawnienie **Datacenter > IBM Data Protection**.

Dla grupy 1 należy przypisać rolę "IBMDDataProtectManage" do centrów przetwarzania danych NewYork_DC i Boston_DC. Dla grupy 2 należy przypisać rolę "IBMDDataProtectManage" do centrów przetwarzania danych LosAngeles_DC i SanFrancisco_DC.

Użytkownicy w każdej grupie mogą używać komponentu wtyczka klienta IBM Spectrum Protect vSphere w kliencie WWW środowiska vSphere do zarządzania maszynami wirtualnymi tylko w odpowiadających im centrach przetwarzania danych.

Problemy związane z niewystarczającymi uprawnieniami

Jeśli użytkownik przeglądarki WWW nie ma wystarczających uprawnień do dowolnego centrum przetwarzania danych, dostęp do widoku jest blokowany. Wyświetlany jest natomiast komunikat o błędzie GVM2013E z informacją, że użytkownik nie jest upoważniony do dostępu do zarządzanych centrów przetwarzania danych ze względu na niewystarczające uprawnienia. Dostępne są też inne nowe komunikaty informujące użytkowników o problemach wynikających z niewystarczających uprawnień. Aby rozwiązać wszelkie problemy związane z uprawnieniami, należy skonfigurować rolę użytkownika zgodnie z opisem w poprzednich sekcjach. Rola użytkownika musi mieć wszystkie uprawnienia określone w tabeli wymaganych uprawnień dla ID użytkownika serwera vCenter i narzędzia przenoszenia danych, a uprawnienia te muszą być stosowane na poziomie centrum przetwarzania danych za pomocą pola wyboru **propagate to children** (propaguj do elementów potomnych).

Jeśli użytkownik komponentu wtyczka klienta IBM Spectrum Protect vSphere nie ma wystarczających uprawnień do centrum przetwarzania danych, funkcje ochrony danych dla tego centrum przetwarzania danych i jego zawartości są niedostępne w rozszerzeniu.

Jeśli ID użytkownika programu IBM Spectrum Protect (określony za pomocą opcji **VMCUser**) ma uprawnienia niewystarczające dla operacji tworzenia i odtwarzania kopii zapasowych, zostanie wyświetlony następujący komunikat:

ANS9365E Błąd interfejsu API VMware vStorage.
"Odmówiono uprawnienia do wykonania tej operacji."

Jeśli ID użytkownika programu IBM Spectrum Protect ma uprawnienia niewystarczające do wyświetlenia maszyny, zostaną wyświetlone następujące komunikaty:

Uruchomiono komendę Backup VM. Łączna liczba maszyn wirtualnych do przetworzenia: 1
ANS4155E Nie można znaleźć maszyny wirtualnej 'tango' na serwerze VMware.
ANS4148E Niepowodzenie tworzenia pełnej kopii zapasowej maszyny wirtualnej 'foxtrot'
z kodem powrotu 4390

Dodatkowe informacje dotyczące wykorzystania uprawnień zawiera serwis WWW **vCenter Server privileges required for the Data Protection for VMware vSphere GUI and data mover**.

Aby za pomocą serwera VMware Virtual Center Server odtworzyć informacje zawarte w dzienniku dotyczące problemów z uprawnieniami, wykonaj następujące kroki:

1. W obszarze vCenter Server Settings (Ustawienia serwera vCenter) wybierz opcję **Logging Options** (Opcje rejestrowania) i dla parametru **vCenter Logging** (Rejestrowanie przez serwer vCenter) ustaw opcję **Trivial (Trivial)**.
2. Ponownie wygeneruj błąd dotyczący uprawnień.
3. Zresetuj parametr **vCenter Logging** (Rejestrowanie serwera vCenter) do jego poprzedniej wartości, aby zapobiec rejestrowaniu w dzienniku nadmiernej ilości informacji.
4. W oknie System Logs (Dzienniki systemowe) znajdź najnowszy dziennik serwera vCenter (vpzd-wxyz.log) i znajdź w nim łańcuch NoPermission. Na przykład:

```
[2011-04-27 15:15:35.955 03756 verbose 'App'] [VpxVmomi] Invoke error:
vim.VirtualMachine.createSnapshot session: 92324BE3-CD53-4B5A-B7F5-96C5FAB3F0EE
Throw: vim.fault.NoPermission
```

Ten komunikat dziennika wskazuje, że ID użytkownika nie miał uprawnień wystarczających do utworzenia obrazu stanu (createSnapshot).

Instalowanie komponentów programu Data Protection for VMware

Można zainstalować wszystkie lub niektóre spośród komponentów, które są dostępne w pakiecie programu Data Protection for VMware dla używanego systemu operacyjnego.

O tym zadaniu

Za pomocą instalatora programu Data Protection for VMware można zainstalować następujące komponenty:

- Agent odtwarzania programu IBM Spectrum Protect
- **Windows** Interfejs wiersza komend agenta odtwarzania
- **Windows** Dokumentacja (plik readme i plik powiadomień)
- Plik zezwolenia programu Data Protection for VMware
- interfejs GUI Data Protection for VMware vSphere
- Składnik narzędzia przenoszenia danych, który zawiera następujące elementy:
 - Interfejs GUI narzędzia przenoszenia danych
 - Klient WWW narzędzie przenoszenia danych
 - Pliki wykonawcze interfejsu API klienta (wersja 64-bitowa)
 - Wiersz komend klienta administracyjnego
 - Pliki wykonawcze interfejsu API VMware vStorage

Można wybrać pełną instalację lub użyć opcji instalacji zaawansowanej, aby zainstalować narzędzie przenoszenia danych (proxy podłączania), agenta odtwarzania i wymagane pakiety obsługi.

Wskazówka: Można utworzyć wiele narzędzi przenoszenia danych w tym samym systemie, w którym znajduje się program Data Protection for VMware, ale można też utworzyć narzędzia przenoszenia danych w systemach zdalnych. Ta konfiguracja zwiększa zasoby dostępne do użycia przez program Data Protection for VMware. Systemy z zainstalowanym narzędziem przenoszenia danych są zwane serwerami kopii zapasowych vStorage.

Uzyskiwanie pakietu instalacyjnego programu Data Protection for VMware

Pakiet instalacyjny programu Data Protection for VMware można pobrać z serwisu pobierania firmy IBM, takiego jak IBM Passport Advantage.

Linux

Zanim rozpocznesz

Jeśli planowane jest pobranie plików, należy ustawić limit użytkownika systemu dotyczący maksymalnej wielkości pliku na brak limitu, aby umożliwić poprawne pobranie plików:

1. Aby sprawdzić maksymalną wielkość pliku, wprowadź następującą komendę:

```
ulimit -Hf
```


2. Jeśli limit użytkownika systemu dotyczący maksymalnej wielkości pliku nie jest ustawiony na brak limitu, zmień go na brak limitu, wykonując instrukcje znajdujące się w dokumentacji używanego systemu operacyjnego.

Procedura

1. Pobierz odpowiedni plik pakietu z jednego z następujących serwisów WWW:
 - W przypadku pierwszej instalacji lub nowej wersji przejdź do programu Passport Advantage pod adresem: <http://www.ibm.com/software/lotus/passportadvantage/>. Passport Advantage to jedyny serwis, z którego można pobrać licencjonowany plik pakietu.
 - Najnowsze informacje, aktualizacje i poprawki serwisowe zawiera serwis wsparcia produktu IBM Spectrum Protect: http://www.ibm.com/support/entry/portal/Overview/Software/Tivoli/Tivoli_Storage_Manager.
2. Jeśli pakiet został pobrany z serwisu pobierania firmy IBM, wykonaj następujące kroki:
 - a. Pobierz plik pakietu do wybranego katalogu. Ścieżka nie może zawierać więcej niż 40 znaków. Rozpakuj pliki instalacyjne do pustego katalogu. Nie należy rozpakowywać plików do katalogu, który zawiera wcześniej rozpakowane pliki lub inne pliki.
 - b. **Linux** Upewnij się, że dla pakietu ustawiono uprawnienie do wykonywania. Jeśli to konieczne, zmień uprawnienia do pliku, wprowadzając następującą komendę:

```
chmod a+x nazwa_pakietu.bin
```
 - c. **Linux** Rozpakuj pakiet, wprowadzając następującą komendę:

```
./nazwa_pakietu.bin
```

gdzie *nazwa_pakietu* jest nazwą pobranego pliku.
 - d. **Windows** Rozpakuj pakiet, dwukrotnie klikając *nazwa_pakietu*, gdzie *nazwa_pakietu* jest nazwą pobranego pliku.

Instalowanie komponentów programu Data Protection for VMware za pomocą kreatora instalacji

Komponenty programu Data Protection for VMware można zainstalować za pomocą kreatora instalacji.

O tym zadaniu

Windows Do zainstalowania programu Data Protection for VMware i narzędzia przenoszenia danych można użyć programu Suite Installer.

Linux Do zainstalowania programu Data Protection for VMware i narzędzia przenoszenia danych można użyć instalatora autonomicznego.

Instalowanie komponentów programu Data Protection for VMware w systemach Windows

Instalowanie komponentów i składników programu Data Protection for VMware za pomocą kreatora instalacji.

Zanim rozpocznieś

Przed zainstalowaniem komponentów programu Data Protection for VMware należy się upewnić, że zostały spełnione następujące wymagania wstępne:

- ID użytkownika z dostępem o uprawnieniach administratora.

- Połączenie sieciowe z serwerem VMware vCenter Server w wersji 6.x (lub nowszej) z dostępem o uprawnieniach administratora.
- Połączenie sieciowe z serwerem IBM Spectrum Protect z dostępem administratora (uprawnienie **System** lub **Nieograniczone uprawnienia do domeny**). Ten serwer musi być dostępny i uruchomiony.
- Należy zapoznać się z następującymi wymaganiami:
 - “Wymagania systemowe” na stronie 12
 - “Uprawnienia wymagane do instalacji” na stronie 16
 - “Wymagane porty komunikacyjne” na stronie 16

Przed zainstalowaniem programu Data Protection for VMware należy wziąć pod uwagę następujące opcje:

Typ instalacji

Instalacja typowa

W przypadku instalacji typowej instalowane są wszystkie komponenty i składniki programu Data Protection for VMware.

Instalacja zaawansowana

Panel instalacji zaawansowanej umożliwia zainstalowanie poszczególnych narzędzi przenoszenia danych. Proces zainstaluje w systemie narzędzie przenoszenia danych (proxy podłączania), agenta odtwarzania i wymagane pakiety obsługi. Tej opcji instalacji należy użyć, aby dodać poszczególne narzędzia przenoszenia danych. Opcja ta instaluje również agenty ochrony aplikacji, aby umożliwić odtwarzanie poszczególnych baz danych. Po instalacji można użyć interfejsu GUI produktu IBM Spectrum Protect do skonfigurowania narzędzia przenoszenia danych i usług za pomocą wtyczki VMware vSphere.

O tym zadaniu

Do zainstalowania programu Data Protection for VMware można użyć programu Suite Installer. Plik `spinstall.exe` dla programu Suite Installer znajduje się w katalogu głównym pakietu instalacyjnego.

Lista komponentów i składników, które można zainstalować, znajduje się w sekcji “Komponenty instalowalne” na stronie 1.

Procedura

Aby zainstalować program Data Protection for VMware, wykonaj następujące kroki z poziomu położenia pliku `spinstall.exe` dla komponentu, który chcesz zainstalować:

1. Kliknij dwukrotnie plik `spinstall.exe`.
2. Postępuj zgodnie z instrukcjami kreatora, aby zainstalować wybrane komponenty.

Co dalej

Aby uzyskać dostęp do interfejsu GUI Data Protection for VMware vSphere, patrz:

- “Uzyskiwanie dostępu do interfejsu GUI Data Protection for VMware vSphere” na stronie 30

Kreator konfiguracji jest automatycznie wyświetlany po pierwszym uruchomieniu interfejsu GUI.

Instalowanie programu Data Protection for VMware w systemach Linux

Instalowanie programu Data Protection for VMware w systemach Linux w trybie programu InstallAnywhere.

Zanim rozpocziesz

Przed zainstalowaniem programu Data Protection for VMware należy się upewnić, że zostały spełnione następujące wymagania wstępne:

- Przed kontynuowaniem należy sprawdzić, czy ID użytkownika ma wymagany poziom uprawnień, a wymagane porty komunikacyjne są otwarte.
- W trakcie procesu instalowania tworzony jest użytkownik **tdpvmware**. Wszystkie komendy **vmcli** należy wprowadzić jako użytkownik **tdpvmware** i z użyciem identyfikatora administratora.
- W przypadku instalacji w trybie konsoli wymagany jest X Window Server.
- Należy zapoznać się z następującymi wymaganiami:
 - “Wymagania systemowe” na stronie 12
 - “Uprawnienia wymagane do instalacji” na stronie 16
 - “Wymagane porty komunikacyjne” na stronie 16

Procedura

Aby zainstalować program Data Protection for VMware, wykonaj następujące działania:

1. W głównym folderze instalacyjnym przejdź do katalogu **CD/Linux/DataProtectionForVMware**.
2. W wierszu komend wprowadź następującą komendę:
`./install-Linux.bin`

Wyniki

Jeśli zostaną wyświetlone ostrzeżenia lub błędy, poszukaj informacji w plikach dzienników. Patrz “Działanie plików dzienników” na stronie 85.

Jeśli nie można zainstalować programu Data Protection for VMware z powodu niepowodzenia, patrz procedura „Ręczne usuwanie programu Data Protection for VMware” w sekcji “Deinstalowanie programu Data Protection for VMware w systemie Linux” na stronie 36.

Wykonywanie czystej instalacji programu Data Protection for VMware w systemie Linux

Jeśli instalacja w systemie Linux zostanie przerwana, zwykle można ją zrestartować. Jeśli jednak zrestartowanie instalacji nie powiedzie się, wymagana będzie nowa (czysta) instalacja.

O tym zadaniu

Przed rozpoczęciem czystej instalacji należy upewnić się, że produkt został usunięty. Aby zapewnić czyste środowisko, wykonaj następujące kroki:

Procedura

1. Jeśli zainstalowany jest interfejs GUI Data Protection for VMware vSphere, wykonaj następujące czynności:

- a. Zatrzymaj interfejs wiersza komend Data Protection for VMware, wprowadzając następującą komendę:
`/etc/init.d/vmcli stop`
- b. Zatrzymaj serwer WWW interfejsu GUI programu Data Protection for VMware, wprowadzając następującą komendę:
`/etc/init.d/webserver stop`
- c. Usuń pakiet .rpm, wprowadzając następującą komendę:
`rpm -e TIVsm-TDPVMwarePlugin`
2. Usuń pozycje produktu mechanizmu wdrażania:
 - a. Aby wyświetlić wszystkie pozycje mechanizmu wdrażania, wprowadź następującą komendę:
`/usr/ibm/common/acsi/bin/de_lsrootiu.sh`
 - b. Aby usunąć wszystkie pozycje mechanizmu wdrażania, wprowadź następującą komendę:
`/usr/ibm/common/acsi/bin/deleteRootIU.sh <UUID> <wyróżnik>`
 - c. Usuń katalog `/var/ibm/common`.
 - d. Usuń katalog `/usr/ibm/common`.
 - e. Wyczyść katalog `/tmp`, usuwając plik `acu_de.log`, jeśli istnieje.
 - f. Usuń katalog `/tmp` zawierający ID użytkownika, który zainstalował mechanizm wdrażania.
 - g. Usuń wszystkie pozycje mechanizmu wdrażania z systemu plików `/etc/inittab`. Pozycje te są ograniczone tekstami `#Begin AC Solution Install block` i `#End AC Solution Install block`. Usuń cały tekst między tymi ogranicznikami, a także sam tekst ograniczników.
 - h. Usuń wszystkie odniesienia mechanizmu wdrażania z systemu plików `/etc/services`.
3. Usuń wszystkie pliki programu Data Protection for VMware z instalacji zakończonej niepowodzeniem:
 - a. Usuń pliki z katalogu `<KATALOG_INSTALACYJNY_UŻYTKOWNIKA>` będącego ścieżką, w której nie powiodło się zainstalowanie programu. Przykład:
`/opt/tivoli/tsm/TDPVMware/`
 - b. Usuń wszystkie skróty na pulpicie.
4. Utwórz kopię zapasową globalnego pliku rejestru (`/var/.com.zerog.registry.xml`). Po utworzeniu kopii zapasowej tego pliku usuń wszystkie znaczniki, które odwołują się do programu Data Protection for VMware.
5. Usuń pliki dzienników w katalogu głównym, które w nazwie zawierają łańcuch TDPVMware. Na przykład:
`IA-TDPVMware-00.log` lub `IA-TDPVMware_Uninstall-00.log`.
6. Usuń użytkownika, który uruchomił interfejs wiersza komend Data Protection for VMware.
 - a. Wprowadź następującą komendę:
`userdel -r tdpvmware`
 - b. Wprowadź następującą komendę:
`groupdel tdpvmware`

Wskazówka: W niektórych wersjach systemu Linux komenda **userdel** usuwa również grupę, gdy nie istnieje żaden inny powiązany z nią użytkownik. W związku z tym należy zignorować wszelkie komunikaty o niepowodzeniu związane z komendą.

Wyniki

Po wykonaniu tych czynności można rozpocząć czystą instalację.

Instalowanie komponentów programu Data Protection for VMware w trybie cichym

Można zainstalować program Data Protection for VMware w tle. Podczas instalacji cichej nie są wyświetlane żadne komunikaty.

O tym zadaniu

Windows Do zainstalowania programu Data Protection for VMware i narzędzia przenoszenia danych można użyć programu Suite Installer.

Linux Do zainstalowania programu Data Protection for VMware i narzędzia przenoszenia danych można użyć instalatora autonomicznego.

Instalowanie programu Data Protection for VMware w systemach Windows w trybie cichym

Instalacja wszystkich komponentów programu Data Protection for VMware i składnika narzędzie przenoszenia danych za pomocą programu Suite Installer w trybie cichym.

Zanim rozpoczniesz

Przed zainstalowaniem programu Data Protection for VMware i składnika narzędzie przenoszenia danych należy się upewnić, że system spełnia wymagania przedstawione w następujących sekcjach:

- “Wymagania systemowe” na stronie 12
- “Uprawnienia wymagane do instalacji” na stronie 16
- “Wymagane porty komunikacyjne” na stronie 16

O tym zadaniu

Ograniczenie: Wszystkie składniki są instalowane w ich lokalizacji domyślnej. Aby znaleźć domyślne katalogi instalacyjne komponentów, patrz tematy podrzędne w sekcji “Komponenty instalowalne” na stronie 1.

Procedura

Aby zainstalować program Data Protection for VMware, wykonaj następujące działania:

1. W wierszu komend wpisz:
`cd wyodrębniony folder\TSMVMWARE_WIN`
2. Wprowadź następującą komendę:

```
spinstall.exe /silent
```

Następujący komunikat jest wyświetlany podczas pierwszego podłączenia woluminu:

Sterownik woluminu wirtualnego nie jest jeszcze zarejestrowany. Agent odtwarzania może zarejestrować ten sterownik teraz. Podczas rejestracji może zostać wyświetlone ostrzeżenie z logo Microsoft Windows. Zaakceptuj to ostrzeżenie, aby dokończyć rejestrowanie. Czy zarejestrować teraz sterownik woluminu wirtualnego?

Aby kontynuować i zarejestrować sterownik woluminu wirtualnego, wpisz **Tak**.

Zadania pokrewne:

“Deinstalowanie programu Data Protection for VMware w systemie Windows w trybie cichym” na stronie 35

Instalowanie programu Data Protection for VMware w systemach Linux w trybie cichym

Istnieje możliwość określenia, które składniki programu Data Protection for VMware zostaną zainstalowane w trybie cichym w systemie operacyjnym Linux.

Zanim rozpocznie

Przed zainstalowaniem programu Data Protection for VMware należy się upewnić, że zostały spełnione następujące wymagania wstępne:

- Przed kontynuowaniem należy sprawdzić, czy ID użytkownika ma wymagany poziom uprawnień, a wymagane porty komunikacyjne są otwarte.
- W trakcie procesu instalowania tworzony jest użytkownik **tdpvmware**. Wszystkie komendy **vmcli** należy wprowadzić jako użytkownik **tdpvmware** i z użyciem identyfikatora administratora.
- W przypadku instalacji w trybie konsoli wymagany jest X Window Server.
- Należy zapoznać się z następującymi wymaganiami:
 - “Wymagania systemowe” na stronie 12
 - “Uprawnienia wymagane do instalacji” na stronie 16
 - “Wymagane porty komunikacyjne” na stronie 16

O tym zadaniu

Program Data Protection for VMware udostępnia następujące składniki do zainstalowania w ramach instalacji cichej dla systemów operacyjnych Linux:

Tabela 7. Składniki instalacji cichej programu Data Protection for VMware

Składnik	Opis	Czy jest instalowany domyślnie?
Docs	Plik readme	Tak
TDPVMwareDM	Instalacja tego składnika obejmuje plik zezwolenia. Umożliwia on programowi IBM Spectrum Protect uruchamianie następujących typów kopii zapasowych: <ul style="list-style-type: none">• Okresowa przyrostowa kopia zapasowa maszyny wirtualnej• Zawsze przyrostowa kopia zapasowa pełnej maszyny wirtualnej• Zawsze przyrostowa - przyrostowa kopia zapasowa maszyny wirtualnej W przypadku nieobciążającego tworzenia kopii zapasowej ten plik musi być zainstalowany na serwerze kopii zapasowych vStorage.	Tak
TDPVMwareGUI	interfejs GUI Data Protection for VMware vSphere. Uwaga: Obejmuje również instalację pliku zezwolenia.	Nie

Procedura

Aby zainstalować program Data Protection for VMware, wykonaj następujące kroki z poziomu katalogu, w którym rozpakowano pakiet instalacyjny:

1. Otwórz plik *ścieżka* `./Linux/DataProtectionForVMware/installer.properties` i usuń oznaczenie komentarza z następującego wpisu, aby zaakceptować licencję (gdzie *ścieżka* oznacza folder instalacyjny):
`LICENSE_ACCEPTED=TRUE`
2. Wybierz jedną z następujących metod, aby zainstalować komponenty programu Data Protection for VMware:
 - W przypadku instalacji domyślnej otwórz folder `CD/Linux/DataProtectionForVMware` i wprowadź następującą komendę:
`./install-Linux.bin -i silent -DLICENSE_ACCEPTED=true`
 - W przypadku instalacji niestandardowej wykonaj następujące kroki:
 - a. Zmodyfikuj plik `installer.properties`, wprowadzając odpowiednie wartości:
 - 1) Podaj ustawienie **INSTALL_MODE=Custom**. Pamiętaj o usunięciu znaku kratki (#) z tej instrukcji.
 - 2) Określ składniki do zainstalowania za pomocą opcji **CHOSEN_INSTALL_FEATURE_LIST**. Na przykład poniższa wartość powoduje zainstalowanie wszystkich składników:
`CHOSEN_INSTALL_FEATURE_LIST=Docs,TDPVMwareDM,TDPVMwareGUI`
 - b. Z poziomu folderu `CD/Linux/DataProtectionForVMware` wprowadź następującą komendę:
`./install-Linux.bin -i silent -f installer.properties`

Pierwsze kroki po zainstalowaniu programu Data Protection for VMware

Po zainstalowaniu programu Data Protection for VMware należy się przygotować do konfigurowania. Preferowaną metodą konfigurowania programu Data Protection for VMware jest użycie kreatora.

Arkusz konfiguracyjny

Ten arkusz umożliwia zapisanie informacji, które są potrzebne podczas konfigurowania programu Data Protection for VMware i administrowania tym programem. Arkusz ułatwia zapamiętanie podanych wartości, gdy konfiguracja zostanie zakończona.

Tabela 8. Arkusz konfiguracyjny programu Data Protection for VMware

Element	Użyta wartość	Uwagi
Informacje o serwerze IBM Spectrum Protect		
Adres serwera IBM Spectrum Protect		
Port serwera IBM Spectrum Protect		
Identyfikator/hasło administratora serwera IBM Spectrum Protect		
Port administracyjny serwera IBM Spectrum Protect		
Opcje definicji węzłów		
Przedrostek do dodania do węzłów		
Domena strategii używana podczas rejestrowania nowych węzłów		
Nazwa/hasło węzła vCenter		

Tabela 8. Arkusz konfiguracyjny programu Data Protection for VMware (kontynuacja)

Element	Użyta wartość	Uwagi
Nazwa/hasło węzła VMCLI		
Nazwy/hasła węzłów centrów przetwarzania danych Zapamiętaj: Można utworzyć wiele węzłów centrów przetwarzania danych.		Nazwa węzła centrum przetwarzania danych składa się z podanego przedrostka, po którym występuje znak podkreślenia, a po nim nazwa centrum przetwarzania danych. Na przykład: <i>PrzedrostekWęzła_NazwaCentrumPrzetwarzaniaDanych</i>
Nazwy/hasła węzłów narzędzia przenoszenia danych na serwerze kopii zapasowych vStorage Zapamiętaj: Można utworzyć wiele węzłów narzędzia przenoszenia danych.		Nazwa węzła narzędzia przenoszenia danych składa się z nazwy węzła centrum przetwarzania danych, po której występuje znak podkreślenia, a po nim łańcuch DM. Na przykład: <i>NazwaWęzłaCentrumPrzetwarzaniaDanych_DM</i>
Nazwy/hasła węzłów narzędzia przenoszenia danych na serwerach zdalnych Zapamiętaj: Można utworzyć wiele węzłów narzędzia przenoszenia danych, które nie znajdują się na serwerze kopii zapasowych vStorage.		
Węzeł proxy podłączania Węzeł proxy podłączania jest używany podczas odtwarzania danych.	Windows: Linux:	

Uzyskiwanie dostępu do interfejsu GUI Data Protection for VMware vSphere

Interfejs GUI Data Protection for VMware vSphere służy do tworzenia i odtwarzania kopii zapasowych maszyn wirtualnych w środowisku VMware vCenter, a także do zarządzania tymi maszynami wirtualnymi.

Zanim rozpoczniesz

Zanim będzie można uzyskać dostęp do interfejsu GUI Data Protection for VMware vSphere, podczas instalacji należy wybrać opcję ochrony danych w środowisku vSphere.

Procedura

- Jeśli podczas instalacji wybrano opcję **Włącz dostęp do interfejsu GUI przez przeglądarkę WWW**, możesz uzyskać dostęp do interfejsu GUI Data Protection for VMware vSphere za pomocą przeglądarki:

- Otwórz przeglądarkę WWW i wprowadź następujący adres URL:

`https://nazwa_hosta:port/TsmVMwareUI`

gdzie:

- nazwa_hosta* oznacza nazwę systemu, w którym zainstalowano interfejs GUI Data Protection for VMware vSphere
- port* oznacza numer portu, na którym interfejs GUI środowiska vSphere jest dostępny. Domyślnym numerem portu jest 9081.

2. Zaloguj się, używając ID użytkownika i hasła vCenter.
- Jeśli podczas instalacji nie wybrano opcji **Włącz dostęp do interfejsu GUI przez przeglądarkę WWW**, możesz uruchomić interfejs GUI Data Protection for VMware vSphere, wykonując następujące kroki:
 1. Otwórz klienta VMware vSphere i zaloguj się, używając ID użytkownika i hasła vCenter.
 2. Na panelu Solutions and Applications (Rozwiązania i aplikacje) klienta vSphere kliknij ikonę interfejsu GUI Data Protection for VMware vSphere.

Aktualizowanie programu Data Protection for VMware

Istnieje możliwość wykonania aktualizacji programu Data Protection for VMware z jego poprzedniej wersji.

Informacje na temat kompatybilności z wcześniejszymi wersjami zawiera nota techniczna 1993819.

Aktualizowanie z wersji 7.1.8: Jeśli podczas procesu aktualizowania zostanie wyświetlony komunikat z pytaniem, czy nadpisać istniejący plik jextract, należy wybrać opcję **Tak dla wszystkich**.

Aktualizowanie programu Data Protection for VMware

Ta procedura zawiera opis aktualizacji do programu Data Protection for VMware 8.1.4.

Zanim rozpocznieś

Ważne: Ta procedura aktualizacji odnosi się do systemu, w którym nie ma zainstalowanego programu IBM Spectrum Protect Snapshot for VMware.

Do przeprowadzenia aktualizacji programu Data Protection for VMware wymagane są uprawnienia administratora.

Aktualizacje istniejącego interfejsu GUI Data Protection for VMware vSphere są przetwarzane w następujący sposób:

- Tworzona jest kopia zapasowa plików parametrów, zanim rozpocznie się proces aktualizowania interfejsu GUI Data Protection for VMware vSphere.
- Używany jest ten sam port bazy danych Derby i domyślny port podstawowy produktu WebSphere Application Server.
- Linux Wartości w profilu (vmclprofile) są używane na potrzeby interfejsu wiersza komend Data Protection for VMware.

Ograniczenie:

- Windows Jeśli program IBM Spectrum Protect for Virtual Environments został zainstalowany w położeniu innym niż domyślne, proces aktualizowania instaluje składniki programu IBM Spectrum Protect for Virtual Environments 8.1.4 w domyślnym katalogu instalacyjnym. Nie można przeprowadzić aktualizacji do położenia innego niż domyślne. Informacje na temat domyślnych katalogów instalacyjnych poszczególnych składników podano w tematach podrzędnych sekcji “Komponenty instalowalne” na stronie 1.
- Linux Windows Proces aktualizowania nie instaluje nowych komponentów. Jeśli na przykład w poprzedniej wersji zainstalowano tylko interfejs GUI agenta odtwarzania, podczas procedury aktualizacji nie zostanie zainstalowany interfejs wiersza

komend agenta odtwarzania. W takim scenariuszu należy ponownie uruchomić program instalacyjny, a następnie wybrać brakujący komponent do zainstalowania.

- **Linux** Wersja agenta odtwarzania w systemie Linux musi być taka sama, jak wersja agenta odtwarzania w proxy Windows. Z tego względu, jeśli wykonywana jest aktualizacja agenta odtwarzania w systemie Linux, należy także zaktualizować wersję agenta odtwarzania w proxy Windows.

Procedura

Aby zaktualizować program Data Protection for VMware, wykonaj następujące kroki:

1. Zatrzymaj wszystkie komponenty i usługi programu Data Protection for VMware, które są uruchomione.
2. Odłącz wszystkie podłączone woluminy wirtualne. Do odłączenia woluminów można użyć interfejsu GUI lub interfejsu wiersza komend agenta odtwarzania (komenda **mount del**).
3. Postępuj zgodnie z instrukcjami podanymi w sekcji “Instalowanie komponentów programu Data Protection for VMware w systemach Windows” na stronie 23.

Uwaga: **Linux** Jeśli zainstalowane jest narzędzie przenoszenia danych w wersji 6.x, należy je zdeinstalować przed zainstalowaniem wersji 8.1.4. Należy postępować zgodnie z instrukcjami w temacie Deinstalowanie klienta programu IBM Spectrum Protect dla systemu Linux x86_64.

4. Pobierz pakiet kodu.
5. W folderze, w którym zapisano pakiet kodu, uruchom proces aktualizacji:
 - a. **Windows** Uruchom plik **spinstall.exe**.
 - b. **Linux** Uruchom plik **install-Linux.bin**.

Na maszynie można zainstalować tylko jeden interfejs GUI Data Protection for VMware vSphere. W związku z tym na jednej maszynie nie jest dozwolony więcej niż jeden interfejs GUI Data Protection for VMware vSphere.

Aktualizowanie programu Data Protection for VMware w 64-bitowym systemie Windows w trybie cichym

Użytkownik może zaktualizować program Data Protection for VMware w trybie cichym w obsługiwanym 64-bitowym systemie operacyjnym.

Zanim rozpoczniesz

Jeśli program Data Protection for VMware w wersji 6.x został zainstalowany w położeniu innym niż domyślne, proces aktualizowania w trybie cichym instaluje składniki programu Data Protection for VMware 8.1.4 w domyślnym katalogu instalacyjnym. Nie można przeprowadzić aktualizacji w trybie cichym do położenia innego niż domyślne. Informacje na temat domyślnych katalogów instalacyjnych poszczególnych składników podano w tematach podrzędnych sekcji “Komponenty instalowalne” na stronie 1.

Procedura

Aby zaktualizować program Data Protection for VMware, wykonaj następujące kroki:

1. Zatrzymaj wszystkie komponenty programu Data Protection for VMware, które są uruchomione.

2. Odłącz wszystkie podłączone woluminy wirtualne. Do odłączenia woluminów można użyć interfejsu GUI lub interfejsu wiersza komend agenta odtwarzania (komenda **mount del**).
3. Odłącz wszystkie podłączone woluminy wirtualne. Do odłączenia woluminów można użyć interfejsu GUI lub interfejsu wiersza komend agenta odtwarzania (komenda **mount del**).
4. Pobierz pakiet kodu.
5. W folderze programu Data Protection for VMware przejdź do folderu X64.
6. W oknie wiersza komend wprowadź następującą komendę:
`spinstall.exe /s /v"/qn REBOOT=ReallySuppress"`

Aktualizowanie programu Data Protection for VMware w systemie Linux w trybie cichym

W tym miejscu podano informacje na temat aktualizowania programu Data Protection for VMware w obsługiwanym systemie operacyjnym Linux w trybie cichym.

O tym zadaniu

Dla składnika instalacji cichej należy użyć następujących parametrów programu Data Protection for VMware:

Tabela 9. Parametry aktualizacji cichej programu Data Protection for VMware

Parametr	Opis	Wartość domyślna
VCENTER_HOSTNAME	Pełna nazwa domenowa lub adres IP serwera vCenter.	Brak
VCENTER_USERNAME	ID użytkownika vCenter. Ten ID użytkownika musi być administratorem VMware, który ma uprawnienie do rejestrowania i wyrejestrowywania rozszerzeń.	Brak
VCENTER_PASSWORD	Hasło vCenter.	Brak
DIRECT_START	Aby uzyskać dostęp do interfejsu GUI Data Protection for VMware vSphere w przeglądarce WWW, należy podać ustawienie DIRECT_START=YES . Interfejs GUI Data Protection for VMware vSphere jest dostępny za pomocą zakładki z adresem URL do serwera WWW interfejsu GUI. Aby interfejs GUI Data Protection for VMware vSphere nie był dostępny za pomocą przeglądarki WWW, należy podać ustawienie DIRECT_START=NO .	YES Ważne: Po zakończeniu aktualizacji wartość parametru DIRECT_START nie może być zmieniona inaczej niż przez reinstalację produktu.

Procedura

Aby zaktualizować program Data Protection for VMware, wykonaj następujące kroki:

1. Upewnij się, że nie ma aktywnej sesji tworzenia kopii zapasowej, odtwarzania ani podłączania.
2. Upewnij się, że zamknięto każdy istniejący interfejs GUI Data Protection for VMware vSphere i interfejs GUI agenta odtwarzania.
3. Pobierz pakiet kodu.
4. Z folderu programu Data Protection for VMware przejdź do folderu Linux.

5. W oknie wiersza komend wprowadź komendę `./install-Linux.bin -i silent -DLICENSE_ACCEPTED=true` z preferowanymi parametrami.
Na przykład:

```
./install-Linux.bin -i silent -LICENSE_ACCEPTED=true  
-VCENTER_HOSTNAME=hostname -VCENTER_USERNAME=username  
-VCENTER_PASSWORD=password  
-DIRECT_START=yes -REGISTER_PLUGIN=yes
```

Deinstalowanie programu Data Protection for VMware

Proces deinstalowania programu Data Protection for VMware jest taki sam dla nowej oraz dla zaktualizowanej wersji.

Deinstalowanie programu Data Protection for VMware w systemie Windows

W tym miejscu podano informacje na temat deinstalowania komponentów programu Data Protection for VMware, usuwania plików i katalogów z systemu Windows.

Zanim rozpocznie

Aby deinstalacja się powiodła, należy skorzystać z następujących wskazówek:

- Jeśli inny interfejs WWW programu Data Protection for VMware udostępnia wtyczkę klienta IBM Spectrum Protect vSphere, nie należy wyrejestrowywać tego rozszerzenia klienta WWW.

O tym zadaniu

Po zakończeniu deinstalacji pliki konfiguracyjne i pliki właściwości znajdują się w katalogu `C:\Program Files\IBM\SpectrumProtect\Framework\VEGUI\config`.

Procedura

1. Zatrzymaj wszystkie komponenty programu Data Protection for VMware, które są uruchomione.
2. Odłącz wszystkie podłączone woluminy wirtualne.
3. Usuń istniejące kopie zapasowe maszyn wirtualnych za pomocą komendy `delete backup` narzędzia przenoszenia danych.
4. Usuń wszystkie zainstalowane usługi narzędzia przenoszenia danych przy użyciu komendy `dsmcutil remove`.

Aby uzyskać listę usług, należy przejść do katalogu `C:\Program Files\Tivoli\TSM\baclient\` i uruchomić komendę `dsmcutil list`.

Usuń usługi przy użyciu komendy podobnej do poniższej, dostosowując nazwę w cudzysłowie do wymienionej usługi:

```
dsmcutil remove /name:"TSM Remote Client Agent"  
dsmcutil remove /name:"TSM Client Acceptor"
```

5. Kliknij kolejno opcje **Start > Panel sterowania > Programy i funkcje > Odinstaluj program**. Odinstaluj następujące programy:
 - Pakiet IBM Spectrum Protect for Virtual Environments Data Protection for VMware
 - Licencja dla produktu IBM Spectrum Protect for Virtual Environments Data Protection for VMware
 - IBM Spectrum Protect JVM

6. Usunąć następujące pliki i katalogi produktu Data Protection for VMware z systemu plików, jeśli istnieją. W przypadku produktu IBM Spectrum Protect for Virtual Environments 8.1.6 i nowszego należy usunąć:

```
C:\IBM\SpectrumProtect
C:\Program Files\IBM\SpectrumProtect
C:\ProgramData\Tivoli\TSM
C:\ProgramData\config
C:\IBM\SpectrumProtect
C:\Program Files\IBM\SpectrumProtect
```

Ponadto można usunąć:

```
C:\Program Files\Tivoli\TSM
```

jeśli pozostałe pliki dziennika i pliki konfiguracyjne nie są już potrzebne. Aby zachować te pliki, należy skopiować je z katalogu C:\Program Files\Tivoli\TSM\baclient. W przypadku produktu IBM Spectrum Protect for Virtual Environments 8.1.4 i wcześniejszego należy usunąć:

```
C:\IBM\tivoli
C:\Program Files (x86)\Common Files\Tivoli\TDPVMware
C:\Program Files\Common Files\Tivoli
C:\ProgramData\Tivoli\TSM
C:\ProgramData\config
```

Ponadto można usunąć:

```
C:\Program Files\Tivoli\TSM
```

jeśli pozostałe pliki dziennika i pliki konfiguracyjne nie są już potrzebne. Aby zachować te pliki, należy skopiować je z katalogu C:\Program Files\Tivoli\TSM\baclient.

Co dalej

Sprawdź, czy wszystkie komponenty zostały usunięte z systemu.

Deinstalowanie programu Data Protection for VMware w systemie Windows w trybie cichym

W tym miejscu podano informacje na temat deinstalowania programu Data Protection for VMware w systemie operacyjnym Windows w trybie cichym.

O tym zadaniu

Po zakończeniu deinstalacji pliki konfiguracyjne i pliki właściwości znajdują się w katalogu C:\Program Files\IBM\SpectrumProtect\Framework\VEGUI\config.

Procedura

Aby zdeinstalować program Data Protection for VMware, wykonaj następujące kroki:

1. Zatrzymaj wszystkie komponenty programu Data Protection for VMware, które są uruchomione.
2. Odłącz wszystkie podłączone woluminy wirtualne. Do odłączenia woluminów można użyć interfejsu GUI lub interfejsu wiersza komend agenta odtwarzania (komenda **mount del**).
3. W wierszu komend wprowadź komendę **cd**, aby przejść do jednego z następujących folderów:
 - Aby dostosować operację deinstalowania, przejdź do folderu X64.

- Aby zdeinstalować program Data Protection for VMware za pomocą programu Suite Installer, przejdź do folderu <folder rozpakowywania>TSM4VE_WIN.
 - 4. W oknie wiersza komend wprowadź następującą komendę:
 - Na potrzeby operacji deinstalacji niestandardowej wybierz jedną z następujących komend:
 - Wprowadź następującą komendę, aby zdeinstalować program Data Protection for VMware i wyrejestrować interfejs GUI Data Protection for VMware vSphere:


```
spinstall.exe /s /v"/qn REBOOT=ReallySuppress REMOVE=ALL
VCENTER_HOSTNAME=<nazwa hosta lub adres IP vCenter>
VCENTER_USERNAME=<nazwa użytkownika vCenter>
VCENTER_PASSWORD=<hasło vCenter>"
```
 - Aby zdeinstalować wszystkie składniki za pomocą programu Suite Installer, wprowadź następującą komendę:


```
spinstall.exe /silent /remove
```
5. Zrestartuj system po zakończeniu deinstalacji.

Deinstalowanie programu Data Protection for VMware w systemie Linux

Deinstalacja programu Data Protection for VMware i usunięcie plików oraz katalogów w obsługiwanym systemie operacyjnym Linux.

Zanim rozpocznie

Aby deinstalacja się powiodła, należy skorzystać z następujących wskazówek:

- Usuń węzły z serwera IBM Spectrum Protect. Należy to zrobić przed przystąpieniem do deinstalacji produktu Data Protection for VMware:
 1. Uruchom komendę `dsmadmc` z katalogu `/opt/tivoli/tsm/client/ba/bin/dsmadmc`.
 2. Może być potrzebne użycie komendy `del` w celu usunięcia obszaru plików dla węzłów: `del file nazwa_węzła *`
 3. Użyj komendy `q`, aby wysłać zapytanie dla węzłów: `q filespace nazwa_węzła *`
 4. Użyj komendy `rem`, aby usunąć węzły: `rem node nazwa_węzła`.
- Zatrzymaj usługi `dsmcad` utworzone dla narzędzia przenoszenia danych. Skorzystaj z instrukcji znajdujących się w nocie technicznej <http://www-01.ibm.com/support/docview.wss?uid=swg21358414>
 1. Użyj komendy `ps`, aby sprawdzić, czy usługa `dsmcad` jest uruchomiona: `ps -ef|grep dsmcad`
 2. Użyj komendy `kill`, aby zatrzymać usługę `dsmcad`: `kill -9 ID_procesu_dsmcad`
- Konieczne jest wyczyszczenie plików związanych z tworzeniem usług przenoszenia danych. Przejdź do katalogu instalacyjnego i uruchom następującą komendę:


```
/opt/tivoli/tsm/client/ba/bin/dsmutilnx cleanupDmFiles 1
```

Naciśnij klawisz Enter, aby wybrać nazwę węzła, a następnie naciśnij klawisz Enter, aby go usunąć.

Nazwy węzłów można znaleźć w pliku `dsm.sys`
- Gdy komponent wtyczka klienta IBM Spectrum Protect vSphere jest deinstalowany ze środowiska VMware vSphere 5.5, usuwane są wyłącznie powiązane opisy i etykiety uprawnień. Rzeczywiste uprawnienia pozostają zainstalowane. Ten problem jest znanym ograniczeniem środowiska VMware. Więcej informacji na ten temat zawiera następujący artykuł z bazy wiedzy środowiska VMware: <http://kb.vmware.com/kb/2004601>.
- Plik zezwolenia produktu Data Protection for VMware nie jest usuwany po zdeinstalowaniu produktu.

O tym zadaniu

Podczas deinstalowania programu Data Protection for VMware w systemie Linux domyślnie typ deinstalacji jest takim samym procesem jak typ pierwotnej instalacji. Aby użyć innego procesu deinstalacji, należy podać poprawny parametr. Jeśli na przykład użyto procesu instalacji cichej, do deinstalacji można użyć kreatora instalacji, podając parametr `-i swing`. Proces deinstalacji należy uruchamiać jako użytkownik root. Należy uzyskać profil użytkownika root. Jeśli użyto komendy `su`, aby przełączyć się do użytkownika root, użyj komendy `su -` do uzyskania profilu użytkownika root.

Gdy proces deinstalacji rozpocznie usuwanie plików programu, anulowanie tego procesu spowoduje, że system nie będzie w stanie czystym. Taka sytuacja może spowodować niepowodzenie przy próbie reinstalacji. W związku z tym należy wyczyścić system, wykonując czynności opisane w sekcji “Ręczne usuwanie programu Data Protection for VMware z systemu Linux”.

Aby zdeinstalować program Data Protection for VMware, wykonaj następujące kroki:

Procedura

1. Przejdź do katalogu zawierającego program deinstalacyjny. Poniższa ścieżka określa domyślne położenie programu deinstalacyjnego: `/opt/tivoli/tsm/tdpvmware/_uninst/TDPVMware/`
2. W zależności od typu instalacji użyj jednej z poniższych metod, aby zdeinstalować program Data Protection for VMware:

Uwaga: Komendy podane w tej procedurze należy wprowadzić w jednym wierszu. W podanych przykładach użyto dwóch wierszy, aby zmieściły się na sformatowanej stronie.

- Aby użyć kreatora instalacji do zdeinstalowania programu Data Protection for VMware, wprowadź następującą komendę:
`./Uninstall_Tivoli_Data_Protection_for_VMware -i swing`
- Aby użyć konsoli do zdeinstalowania programu Data Protection for VMware, wprowadź następującą komendę:
`./Uninstall_Tivoli_Data_Protection_for_VMware -i console`
- Aby zdeinstalować program Data Protection for VMware w trybie cichym, wprowadź następującą komendę:
`./Uninstall_Tivoli_Data_Protection_for_VMware -i silent
-f uninstall.properties`

Plik `uninstall.properties` zawiera informacje o połączeniu z serwerem vCenter. Te informacje są potrzebne do zdeinstalowania interfejsu GUI Data Protection for VMware vSphere.

Ręczne usuwanie programu Data Protection for VMware z systemu Linux

O tym zadaniu

Jeśli nie można zdeinstalować programu Data Protection for VMware za pomocą standardowej procedury deinstalacji, należy ręcznie usunąć program Data Protection for VMware z systemu, jak to opisano w poniższych krokach. Ten proces należy wykonać jako użytkownik root.

Procedura

1. Jeśli zainstalowano interfejs GUI Data Protection for VMware vSphere, należy usunąć jego pakiet z bazy danych menedżera pakietów za pomocą następującej komendy:

- ```
rpm -e TIVsm-TDPVMwarePlugin
```
2. Usuń interfejs API programu IBM Spectrum Protect za pomocą następującej komendy:
 

```
rpm -e TIVsm-API64
gskssl64.linux.x86_64.rpm
skcrypt64.linux.x86_64
TIVsm-TDPVMwarePlugin.x86_64.rpm
TIVsm-DPAPI.x86_64.rpm
```
  3. Usuń pozycje produktu z mechanizmu wdrażania:
    - a. Wprowadź następującą komendę, aby wyświetlić listę wszystkich pozycji:
 

```
/usr/ibm/common/acs/bin/de_lsrootiu.sh
```
    - b. Wprowadź następującą komendę, aby usunąć pozycje zainstalowanych jednostek związane z produktem Data Protection for VMware:
 

```
/usr/ibm/common/acs/bin/deleteRootIU.sh <UUID> <wyróżnik>
```

Upewnij się, że zostały usunięte pozycje następujących jednostek:

```
FBJRE
TDPVMwareGUI
JavaHelp
TDPVMwareDM
```

Po zakończeniu deinstalacji należy usunąć następujące katalogi, jeśli istnieją:

    - /opt/tivoli/tsm/client
    - /opt/tivoli/tsm/tdpvmware

Usuń użytkownika tdpvmware i powiązane katalogi:

    - userdel tdpvmware
    - /home/tdpvmware
    - /etc/adsm
  4. Utwórz kopię zapasową globalnego pliku rejestru (/var/.com.zerog.registry.xml). Po utworzeniu kopii zapasowej tego pliku usuń wszystkie znaczniki powiązane z programem Data Protection for VMware.
  5. Usuń wszystkie pliki z katalogu instalacyjnego (/opt/tivoli/tsm/tdpvmware). Ponadto usuń wszystkie skróty znajdujące się na pulpicie.
  6. Utwórz kopię zapasową plików dzienników znajdujących się w katalogu /root, które w nazwie pliku zawierają łańcuch TDPVMware. Przykład: IA-TDPVMware-00.log lub IA-TDPVMware\_Uninstall-00.log. Usuń te pliki dzienników po utworzeniu ich kopii zapasowej. Usuwanie je, można sprawdzić wszelkie błędy wygenerowane w przypadku ponownego niepowodzenia procesu instalowania.
  7. Teraz możesz ponownie zainstalować produkt zgodnie z opisem w sekcji “Instalowanie programu Data Protection for VMware w systemach Linux” na stronie 25.

---

## Modyfikowanie istniejącej instalacji produktu Data Protection for VMware

W tej sekcji przedstawiono instrukcje dotyczące modyfikowania pakietów i składników w istniejącej instalacji produktu Data Protection for VMware.

Przy użyciu programu Suite Installer można zmienić bazowe pakiety, które są zainstalowane w systemie. Aby zmodyfikować dowolne funkcje poszczególnych pakietów, można użyć panelu sterowania Windows **Programy i funkcje**.



## Modyfikowanie pakietów w istniejącej instalacji produktu Data Protection for VMware

Do wprowadzenia zmian w istniejącej instalacji produktu Data Protection for VMware można użyć programu Suite Installer.

### Zanim rozpocznieš

Sprawdź, czy masz nośnik źródłowy przed użyciem programu instalacyjnego pakietu. Plik `spinstall.exe` dla programu Suite Installer znajduje się w katalogu głównym pakietu instalacyjnego.

### O tym zadaniu

Użyj programu Suite Installer, aby zmodyfikować pakiety, które są zainstalowane w istniejącej instalacji produktu Data Protection for VMware. Można dodać lub usunąć:

- Narzędzie przenoszenia danych
- Data Protection for VMware

Wykonaj następujące kroki:

### Procedura

1. Kliknij dwukrotnie plik `spinstall.exe`, aby uruchomić pakiet instalatora pakietu.
2. Użyj pól wyboru pakietów w panelu **Konfiguracja niestandardowa**, aby określić pakiety, które należy zainstalować.
3. Wybierz pakiety wymagane dla tej instalacji.

## Modyfikowanie składników w istniejącej instalacji produktu Data Protection for VMware

Można użyć funkcji Panelu Sterowania systemu Windows i panelu zarządzania opcjami, aby wprowadzić zmiany w opcjach dla istniejącej instalacji produktu Data Protection for VMware.

### Zanim rozpocznieš

Sprawdź, czy masz nośnik źródłowy przed zmodyfikowaniem pakietu instalacyjnego.

### O tym zadaniu

Użyj usługi Windows, aby zmodyfikować poszczególne funkcje pakietu, które są dostępne w istniejącej instalacji produktu Data Protection for VMware. Można wybrać opcję zmodyfikowania następujących składników:

- Narzędzie przenoszenia danych
- Data Protection for VMware

Wykonaj następujące kroki:

### Procedura

1. W sekcji **Programy i funkcje** okna **Panel sterowania** systemu Windows, kliknij prawym przyciskiem myszy aplikację IBM Spectrum Protect for Virtual Environments: Data Protection for VMware.
2. Kliknij przycisk **Modyfikuj**, aby zaktualizować listę aktualnie zainstalowanych składników pakietu.

3. Wybierz opcje wymagane dla tej instalacji.

---

## Rozdział 2. Konfigurowanie programu Data Protection for VMware

Ta sekcja zawiera instrukcje dotyczące konfigurowania programu Data Protection for VMware i uruchamiania powiązanych z nim usług.

---

### Konfigurowanie nowej instalacji za pomocą kreatora

Do konfiguracji początkowej lub wprowadzenia mniej istotnych zmian użyj kreatora konfiguracji.

#### Zanim rozpocznieś

System, w którym zainstalowano program Data Protection for VMware, musi mieć połączenie sieciowe z następującymi serwerami:

- Serwer vStorage Backup Server
- Serwer IBM Spectrum Protect
- Serwer vCenter

#### O tym zadaniu

Aby skonfigurować środowisko programu Data Protection for VMware, wykonaj następujące kroki:

#### Procedura

1. Otwórz przeglądarkę WWW i wprowadź adres serwera WWW interfejsu GUI. Na przykład:  
`https://guihost.mycompany.com:9081/TsmVMwareUI/`
  - W środowisku vSphere zaloguj się, używając nazwy i hasła użytkownika serwera vCenter.
2. W oknie Pierwsze kroki przejdź do okna Konfiguracja i kliknij opcję **Uruchom kreatora konfiguracji**.
3. Postępuj zgodnie z instrukcjami wyświetlanymi na każdej stronie kreatora, aż zostanie wyświetlone okno Podsumowanie. Przejrzyj ustawienia i kliknij przycisk **Zakończ**, aby dokończyć konfigurowanie i wyjść z kreatora.

**Wskazówka:** Informacje na temat każdej strony konfiguracji znajdują się w pomocy elektronicznej, która jest instalowana z interfejsem GUI. Kliknięcie opcji **Dowiedz się więcej** w dowolnym oknie interfejsu GUI powoduje otwarcie pomocy elektronicznej zapewniającej asystę do wykonywanych czynności. Więcej informacji znajduje się w temacie *Uruchamianie kreatora konfiguracji*.

4. Sprawdź, czy węzły narzędzia przenoszenia danych są skonfigurowane poprawnie:
  - a. Kliknij kartę **Konfiguracja**, aby wyświetlić stronę Status konfiguracji.
  - b. Na stronie Status konfiguracji wybierz węzeł narzędzia przenoszenia danych, aby wyświetlić informacje o jego statusie na panelu Szczegóły statusu. Gdy węzeł wyświetla ostrzeżenie lub komunikat o błędzie, kliknij ten węzeł i użyj informacji dostępnych na panelu Szczegóły statusu, aby rozwiązać problem. Następnie wybierz węzeł i kliknij opcję **Sprawdź poprawność wybranego węzła**, aby upewnić się, że problem został rozwiązany. Kliknij przycisk **Odśwież**, aby ponownie przetestować wszystkie węzły.

## Wyniki

**Krótką ścieżką:** Po pomyślnym wykonaniu tego zadania konfiguracyjnego nie są wymagane żadne dodatkowe czynności konfiguracyjne w celu tworzenia kopii zapasowych danych maszyn wirtualnych.

---

## Używanie notatnika do edytowania istniejącej instalacji

Ten notatnik służy do edycji istniejących ustawień konfiguracyjnych.

### Zanim rozpoczniesz

Notatnik Edytuj konfigurację umożliwia wykonanie następujących czynności dla istniejącej konfiguracji:

- Ustawienie lub zmiana ID administratora programu IBM Spectrum Protect.
- Zresetowanie hasła i odblokowanie węzła VMCLI.
- (Środowisko vSphere) Dodanie centrów przetwarzania danych VMware do domeny interfejsu GUI Data Protection for VMware vSphere lub ich usunięcie z tej domeny.
- Dodanie lub usunięcie węzłów proxy podłączania. Zmodyfikowanie hasła dla istniejącego węzła proxy podłączania.
- Dodanie lub usunięcie węzłów narzędzia przenoszenia danych. Zmodyfikowanie hasła dla istniejącego węzła narzędzia przenoszenia danych.
- Włączenie odtwarzania plików.
- Włączenie obsługi znaczników dla węzła narzędzia przenoszenia danych.

### O tym zadaniu

Aby edytować istniejącą konfigurację, wykonaj następujące kroki:

#### Procedura

1. Otwórz przeglądarkę WWW i wprowadź adres serwera WWW interfejsu GUI. Na przykład:  
`https://guihost.mycompany.com:9081/TsmVMwareUI/`  
  
Zaloguj się, używając nazwy użytkownika i hasła vCenter.
2. W oknie Pierwsze kroki przejdź do okna Konfiguracja i kliknij opcję **Edytuj konfigurację**.
3. Przejdź do strony właściwej dla czynności edycji i postępuj zgodnie z instrukcjami. Musisz kliknąć przycisk **OK**, aby zapisać zmiany, zanim przejdiesz do kolejnej strony Ustawienia konfiguracyjne. W przeciwnym razie wprowadzone zmiany nie odniosą skutku.

**Ważne:** Informacje na temat każdej strony konfiguracji znajdują się w pomocy elektronicznej, która jest instalowana z interfejsem GUI. Kliknięcie opcji **Dowiedz się więcej** w dowolnym oknie interfejsu GUI powoduje otwarcie pomocy elektronicznej zapewniającej asystę do wykonywanych czynności. Patrz temat *Edytowanie istniejącej konfiguracji*.

## Wyniki

Zaktualizowane ustawienia są wyświetlane w oknie Konfiguracja.

---

## Włączanie w środowisku obsługi odtwarzania plików

### Windows

Po włączeniu przez administratora funkcji odtwarzania plików właściciele plików mogą odtwarzać pliki bez jego asysty.

### Zanim rozpocznieś

Jeśli nie sprawdzono, czy wszystkie wymagania wstępne zostały spełnione, należy przejrzeć temat dotyczący wymagań wstępnych dla odtwarzania plików w publikacji *IBM Spectrum Protect for Virtual Environments: Data Protection for VMware – Podręcznik użytkownika*.

### O tym zadaniu

Wykonaj następujące kroki w systemie, w którym zainstalowano interfejs GUI Data Protection for VMware vSphere.

### Procedura

1. Uruchom interfejs GUI Data Protection for VMware vSphere, otwierając przeglądarkę WWW i wprowadzając adres serwera WWW interfejsu GUI. Na przykład:

`https://<adres webGUI>:9081/TsmVMwareUI/`

Zaloguj się, używając ID użytkownika i hasła vCenter.

2. W oknie Pierwsze kroki kliknij opcję **Konfiguracja** i wybierz jedno z następujących zadań na liście Zadania:
  - Jeśli konfigurujesz nowe środowisko, wykonaj następujące kroki:
    - a. Wybierz opcję **Uruchom kreatora konfiguracji klienta**.
    - b. Postępuj zgodnie z instrukcjami wyświetlanymi na każdej stronie kreatora. Użyj następujących wskazówek, aby wypełnić stronę Odtwarzanie plików:
      - 1) Wybierz opcję **Włącz odtwarzanie plików**.
      - 2) Zmodyfikuj informacje kontaktowe administratora wyświetlane w interfejsie dla odtwarzania plików. Jeżeli nie chcesz podawać informacji kontaktowych, anuluj zaznaczenie tego pola wyboru.
      - 3) Jeśli w danym środowisku używane są kopie zapasowe maszyn wirtualnych z systemem Windows, podaj informacje autoryzacyjne administratora domeny Windows. W przeciwnym razie anuluj zaznaczenie pola wyboru i nie podawaj żadnych informacji autoryzacyjnych.

**Wskazówka:** Operacja odtwarzania pliku używa informacji autoryzacyjnych administratora domeny, aby uzyskać dostęp do zasobów sieciowych zdalnej maszyny wirtualnej. Operacja zakończy się niepowodzeniem, jeśli w danym środowisku używane są kopie zapasowe maszyn wirtualnych z systemem Windows i nie zostaną podane informacje autoryzacyjne (lub będą one niepoprawne). Dlatego należy anulować zaznaczenie pola wyboru, jeśli nie ma kopii zapasowych maszyn wirtualnych z systemem Windows.

- 4) Kliknij adres URL interfejsu odtwarzania plików, aby sprawdzić, czy interfejs jest dostępny.

**Zapamiętaj:** Zanotuj adres URL interfejsu odtwarzania plików. Właściciel maszyny wirtualnej może uzyskać dostęp do interfejsu odtwarzania plików za pośrednictwem tego adresu URL.

- 5) Kliknij przycisk **OK**, aby zapisać zmiany.

- Jeśli aktualizujesz istniejące środowisko, wykonaj następujące kroki:
  - a. Wybierz opcję **Edytuj konfigurację TSM**.
  - b. Na stronie Odtwarzanie plików użyj następujących wskazówek:
    - 1) Wybierz opcję **Włącz odtwarzanie plików**.
    - 2) Zmodyfikuj informacje kontaktowe administratora wyświetlane w interfejsie dla odtwarzania plików. Jeżeli nie chcesz podawać informacji kontaktowych, anuluj zaznaczenie tego pola wyboru.
    - 3) Jeśli w danym środowisku używane są kopie zapasowe maszyn wirtualnych z systemem Windows, podaj informacje autoryzacyjne administratora domeny Windows. W przeciwnym razie anuluj zaznaczenie pola wyboru i nie podawaj żadnych informacji autoryzacyjnych.

**Wskazówka:** Operacja odtwarzania pliku używa informacji autoryzacyjnych administratora domeny, aby uzyskać dostęp do zasobów sieciowych zdalnej maszyny wirtualnej. Operacja zakończy się niepowodzeniem, jeśli w danym środowisku używane są kopie zapasowe maszyn wirtualnych z systemem Windows i nie zostaną podane informacje autoryzacyjne (lub będą one niepoprawne). Dlatego należy anulować zaznaczenie pola wyboru, jeśli nie ma kopii zapasowych maszyn wirtualnych z systemem Windows.

- 4) Kliknij adres URL interfejsu odtwarzania plików, aby sprawdzić, czy interfejs jest dostępny.

**Zapamiętaj:** Zanotuj adres URL interfejsu odtwarzania plików. Właściciel maszyny wirtualnej może uzyskać dostęp do interfejsu odtwarzania plików za pośrednictwem tego adresu URL.

- 5) Kliknij przycisk **OK**, aby zapisać zmiany.

## Wyniki

Środowisko jest gotowe do wykonywania operacji odtwarzania plików. Właściciele plików mogą odtwarzać własne pliki, podając adres URL interfejsu odtwarzania plików produktu IBM Spectrum Protect.

## Konfigurowanie operacji odtwarzania plików w systemie Linux

### Linux

Aby włączyć składnik odtwarzania plików, gdy program Data Protection for VMware jest zainstalowany w systemie Linux, w systemie Windows należy skonfigurować dodatkowe środowisko programu Data Protection for VMware.

### O tym zadaniu

Gdy program Data Protection for VMware jest uruchamiany w środowisku systemu Linux, składnik odtwarzania plików musi być zainstalowany w systemie Windows, aby aktywować ten składnik.

### Procedura

1. Skonfiguruj oddzielny serwer Windows używany na potrzeby składnika odtwarzania plików.
2. Zainstaluj program Data Protection for VMware w systemie Windows. Podczas instalacji zaakceptuj wartości domyślne.
3. Podczas konfigurowania programu Data Protection for VMware w systemie Windows użyj następujących nazw węzłów:

- a. Utwórz węzeł serwera vCenter o nazwie VCENTER\_FR.
  - b. Utwórz węzeł interfejsu VMCLI o nazwie VMCLI\_FR.
  - c. Wykorzystaj nazwę węzła centrum przetwarzania danych w środowisku Linux. Na przykład: DATACENTER.
  - d. Nie twórz węzła narzędzia przenoszenia danych. Węzeł narzędzia przenoszenia danych nie jest wymagany dla funkcji odtwarzania plików w tym scenariuszu.
  - e. Utwórz następujące nowe pary węzłów proxy podłączania o nazwach REMOTE\_FR\_MP\_WIN i REMOTE\_FR\_MP\_LNX.
4. Na stronie Odtwarzanie plików kreatora konfiguracji wybierz opcję **Włącz odtwarzanie plików**.
  5. Aby uzyskać dostęp do interfejsu odtwarzania plików, otwórz przeglądarkę WWW i wprowadź adres URL podany przez administratora. Na przykład:  
https:\\nazwa\_hosta:9081\FileRestoreUI

gdzie nazwa\_hosta oznacza nazwę hosta systemu Windows, w którym zainstalowano program Data Protection for VMware.

## Wyniki

W poniższym przykładzie przedstawiono relacje węzłów proxy na serwerze IBM Spectrum Protect:

tsm: SERVER>q proxy

| Węzeł docelowy | Węzeł agenta                      |
|----------------|-----------------------------------|
| VCENTER        | VMCLI DATACENTER                  |
| VCENTER_FR     | VMCLI_FR DATACENTER               |
| DATACENTER     | VMCLI_VMCLI_FR                    |
|                | DATAMOVER1                        |
|                | REMOTE_MP_WIN REMOTE_MP_LNX       |
|                | REMOTE_FR_MP_WIN REMOTE_FR_MP_LNX |

Węzły dodatkowe, które są tworzone, aby włączyć funkcję odtwarzania plików, mają przyrostek \_FR.

## Modyfikowanie opcji na potrzeby operacji odtwarzania plików

### Windows

Aby umożliwić administratorom konfigurowanie przetwarzania związanego z odtwarzaniem i sterowanie nim na potrzeby operacji odtwarzania plików, zmodyfikuj opcje w pliku frConfig.props.

## O tym zadaniu

Wykonaj następujące kroki w systemie, w którym zainstalowano interfejs GUI Data Protection for VMware vSphere.

## Procedura

1. Przejdź do katalogu, w którym znajduje się plik frConfig.props. Na przykład otwórz wiersz komend i wprowadź następującą komendę:  
cd C:\IBM\SpectrumProtect\webserver\usr\servers\veProfile\tsmVmGUI
2. Otwórz plik frConfig.props w edytorze tekstu w trybie administratora i zmodyfikuj opcje odpowiednio do potrzeb. Użyj informacji z sekcji “Opcje odtwarzania plików” na stronie 46, aby określić opcje do zmodyfikowania.

3. Zapisz zmiany i zamknij plik `frConfig.props`.

## Wyniki

Zmodyfikowane opcje są stosowane do interfejsu odtwarzania plików programu IBM Spectrum Protect.

## Opcje odtwarzania plików

Opcje znajdujące się w pliku `frConfig.props` służą do sterowania konfiguracją, obsługą i przetwarzaniem odtwarzania na potrzeby operacji odtwarzania plików.

### **`enable_contact_info=false | true`**

Określ, czy podać informacje kontaktowe administratora, aby właściciele plików mogli uzyskać wsparcie.

#### **false**

Właściciele plików nie otrzymują informacji kontaktowych administratora. Jest to wartość domyślna.

#### **true**

Właściciele plików otrzymują informacje kontaktowe administratora.

Jeśli zostanie określone ustawienie **`enable_contact_info=true`**, należy podać informacje w opcji **`contact_info`**.

### **`enable_filerstore=false | true`**

Określ, czy właściciele plików mogą odtwarzać własne pliki z maszyny wirtualnej za pomocą interfejsu odtwarzania plików programu IBM Spectrum Protect.

#### **false**

Właściciele plików nie mogą odtwarzać własnych plików za pomocą interfejsu odtwarzania plików programu IBM Spectrum Protect. Jest to wartość domyślna.

#### **true**

Właściciele plików mogą odtwarzać własne pliki za pomocą interfejsu odtwarzania plików programu IBM Spectrum Protect.

### **`maximum_mount_points=liczba_punktów_odtwarzania`**

Podaj maksymalną liczbę punktów odtwarzania, które są jednocześnie dostępne do konta użytkownika. Wartością minimalną jest 1 punkt odtwarzania. Wartość maksymalna wynosi 256 punktów podłączenia. Wartością domyślną są 2 punkty podłączenia.

**Wskazówka:** Aby zapobiec wielokrotnemu podłączaniu maszyny wirtualnej na potrzeby jednoczesnych operacji odtwarzania, dla tej opcji należy ustawić niską wartość.

### **`mount_session_timeout_minutes=liczba_minut`**

Podaj czas (w minutach), przez jaki operacja odtwarzania i podłączony punkt odtwarzania mogą pozostawać bezczynne, zanim sesja zostanie anulowana. Anulowanie powoduje odłączenie punktu odtwarzania. Wartość maksymalna wynosi 8 godzin (480 minut). Wartością domyślną jest 30 minut.

**Wskazówka:** Aby zapobiec nieoczekiwanemu anulowaniu sesji, należy zwiększyć liczbę minut.

### **`restore_info_duration_hours=liczba_godzin`**

Podaj czas (w godzinach), przez jaki informacje o ostatnich działaniach związanych z odtwarzaniem są przechowywane w interfejsie odtwarzania plików programu IBM Spectrum Protect. Okno działań związanych z odtwarzaniem umożliwia sprawdzenie informacji o błędach i ostatnio zakończonych zadaniach. Informacje te umożliwiają



znalezienie ostatnio odtworzonych plików. Maksymalna wartość to 336 godzin (14 dni). Wartość domyślna to 168 godzin (jeden tydzień).

#### **contact\_info=informacje o administratorze**

Podaj informacje kontaktowe administratora, aby właściciele plików mogli uzyskać wsparcie. Informacje kontaktowe są wyświetlane w interfejsie odtwarzania plików programu IBM Spectrum Protect w następujących miejscach:

- Okno logowania
- Panel Informacje o w menu pomocy
- Odsyłacz do informacji na temat wsparcia w komunikatach interfejsu

Za pomocą kreatora konfiguracji interfejsu GUI Data Protection for VMware vSphere lub notatnika można nadpisać następujące opcje:

- **enable\_contact\_info**
- **enable\_filerestore**
- **contact\_info**

---

## **Konfigurowanie aktywności dziennika dla operacji odtwarzania plików**

Aby umożliwić administratorom konfigurowanie formatowania i rejestrowania treści na potrzeby operacji odtwarzania plików, zmodyfikuj opcje w pliku FRLog.config.

### **Zanim rozpocznieś**

Plik FRLog.config jest generowany przy pierwszym dostępie do interfejsu odtwarzania plików programu IBM Spectrum Protect.

### **O tym zadaniu**

Wykonaj następujące kroki w systemie, w którym zainstalowano interfejs GUI Data Protection for VMware vSphere.

### **Procedura**

1. Przejdź do katalogu, w którym znajduje się plik FRLog.config. Otwórz wiersz komend i wprowadź następującą komendę:  
`cd C:\IBM\SpectrumProtect\webserver\usr\servers\veProfile\frGUI\`
2. Otwórz plik FRLog.config w edytorze tekstu w trybie administratora i zmodyfikuj opcje odpowiednio do potrzeb. Użyj informacji z sekcji “Opcje aktywności dziennika odtwarzania plików” na stronie 48, aby określić opcje do zmodyfikowania.
3. Zapisz zmiany i zamknij plik FRLog.config.
4. Zrestartuj serwer WWW interfejsu GUI:
  - a. Kliknij kolejno opcje **Start > Panel sterowania > Narzędzia administracyjne > Usługi**.
  - b. Prawym przyciskiem myszy kliknij pozycję **Data Protection for VMware Web Server Service** (Usługa serwera WWW programu Data Protection for VMware), a następnie kliknij opcję **Zrestartuj**.

### **Wyniki**

Ustawienia są stosowane do zawartości i formatu informacji rejestrowanych w związku z operacjami odtwarzania plików.

## Opcje aktywności dziennika odtwarzania plików

Opcje znajdujące się w pliku FRLog.config służą do sterowania zawartością i formatem informacji rejestrowanych w związku z operacjami odtwarzania plików.

Następujące opcje służą do rejestrowania informacji dla zadań odtwarzania plików w pliku fr\_gui.log:

### **MAX\_LOG\_FILES=*liczba***

Podaj maksymalną liczbę plików fr\_gui.log, które mają być przechowywane. Wartością domyślną jest 8.

### **MAX\_LOG\_FILE\_SIZE=*liczba***

Podaj maksymalną wielkość pliku fr\_gui.log wyrażoną w kB. Wartością domyślną jest 8192 kB.

Następujące opcje służą do rejestrowania informacji dla usług odtwarzania plików w pliku fr\_api.log. Usługi te są wewnętrznymi usługami interfejsu API powiązanymi z działaniami odtwarzania plików:

### **API\_MAX\_LOG\_FILES=*liczba***

Podaj maksymalną liczbę plików fr\_api.log, które mają być przechowywane. Wartością domyślną jest 8.

### **API\_MAX\_LOG\_FILE\_SIZE=*liczba***

Podaj maksymalną wielkość pliku fr\_api.log wyrażoną w kB. Wartością domyślną jest 8192 kB.

### **API\_LOG\_FILE\_NAME=*nazwa pliku dziennika\_API***

Podaj nazwę pliku dziennika interfejsu API. Wartością domyślną jest fr\_api.log.

### **API\_LOG\_FILE\_LOCATION=*nazwa pliku dziennika\_API***

Podaj położenie pliku dziennika interfejsu API. Położenie musi być określone przy użyciu ukośnika (/). Domyślne położenie to C:/IBM/SpectrumProtect/webserver/usr/servers/veProfile/logs.

### **FR.API.LOG=ON | OFF**

Określ, czy włączyć rejestrowanie dla usług odtwarzania plików.

- Aby włączyć rejestrowanie dla usług odtwarzania plików, podaj wartość ON. Wartością domyślną jest ON.
- Aby wyłączyć rejestrowanie dla usług odtwarzania plików, podaj wartość OFF.

Informacje na temat rozwiązywania problemów, które mogą wystąpić podczas operacji odtwarzania plików, zawiera sekcja Opcje śledzenia dla odtwarzania plików. W pliku FRLog.config znajdują się także opcje śledzenia.

---

## Konfigurowanie węzła narzędzia przenoszenia danych do obsługi znaczników

Jeśli obsługa znaczników jest włączona w węźle narzędzia przenoszenia danych, administratorzy mogą stosować znaczniki ochrony danych do obiektów spisu zasobów w VMware vCenter.

### Zanim rozpocznie

Sprawdź, czy spełnione są następujące wymagania:

- Serwer VMware vCenter musi być w wersji 6.0 Update 1 lub nowszej.

- Aby interfejs GUI programu Data Protection for VMware vSphere działał poprawnie z obsługą znaczników, podczas instalowania tego interfejsu GUI należy się upewnić, że zostały spełnione następujące wymagania:
  - Co najmniej jedno narzędzie przenoszenia danych i interfejs GUI programu Data Protection for VMware vSphere muszą być zainstalowane na tym samym serwerze. Ten węzeł narzędzia przenoszenia danych musi być skonfigurowany w taki sposób, aby informacje autoryzacyjne serwera vCenter były zapisywane. Informacje autoryzacyjne można zapisywać przez uruchomienie kreatora konfiguracji w celu zapisania hasła węzła narzędzia przenoszenia danych lub przez użycie komendy **dsrmc set password** w wierszu komend narzędzia przenoszenia danych.  
 Jeśli używane są inne narzędzia przenoszenia danych, uruchamiane w maszynach wirtualnych lub maszynach fizycznych jako dodatkowe narzędzia przenoszenia danych, można je zainstalować na innych serwerach. W celu zapewnienia obsługi znaczników wszystkie te narzędzia przenoszenia danych muszą być skonfigurowane z użyciem opcji **VMTAGDATAMOVER YES**. Te dodatkowe narzędzia przenoszenia danych nie wymagają zainstalowania interfejsu GUI programu Data Protection for VMware vSphere na tym samym serwerze, aby mogły działać poprawnie jako narzędzia przenoszenia danych obsługujące znaczniki.
  - **Linux** Dla narzędzia przenoszenia danych w systemie Linux należy podać w zmiennej środowiskowej **LD\_LIBRARY\_PATH** katalog instalacyjny narzędzia przenoszenia danych oraz katalog zawierający bibliotekę współużytkowaną **libjvm.so** środowiska Java™. Ścieżka pliku **libjvm.so** jest używana do obsługi znaczników, gdy w narzędziu przenoszenia danych zostanie ustawiona opcja **vmtagdatamover**. Odpowiednie instrukcje zawiera sekcja Konfigurowanie węzłów narzędzia przenoszenia danych w środowisku vSphere.
  - **Linux** W systemach operacyjnych Linux interfejs GUI programu Data Protection for VMware vSphere musi być zainstalowany z użyciem domyślnej nazwy użytkownika (**tdpvmware**).
  - W klientach systemów UNIX i Linux istniejące hasła w plikach **TSM.PWD** są migrowane do nowej składnicy haseł w tym samym położeniu. Dla administratorów domyślnym położeniem składnicy haseł jest **/etc/adsm**. Dla użytkowników innych niż root położenie składnicy haseł jest podane w opcji **passworddir**.  
 Po migracji plik **TSM.PWD** jest usuwany.

**Uwaga:** Dodatkowe informacje dotyczące wykorzystania uprawnień wymaganych do pracy ze znacznikami zawiera serwis WWW Installing the Data Protection for VMware components

## O tym zadaniu

Znaczniki ochrony danych są używane do konfigurowania strategii kopii zapasowych maszyn wirtualnych w obiektach spisu zasobów VMware. Te znaczniki ochrony danych są prezentowane jako ustawienia, które można zmieniać w komponencie wtyczka klienta IBM Spectrum Protect vSphere.

## Procedura

Użyj jednej z poniższych metod:

| Opcja                                                                                          | Opis                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Aby skonfigurować węzeł narzędzia przenoszenia danych za pomocą interfejsu GUI wtyczki vSphere | <ol style="list-style-type: none"><li>1. Z poziomu wtyczki vSphere wybierz program IBM Spectrum Protect.</li><li>2. Na karcie <b>Konfiguracja</b> wybierz opcję <b>Narzędzia przenoszenia danych</b>.</li><li>3. W panelu <b>Dodaj narzędzie przenoszenia danych</b> wybierz centrum przetwarzania danych z rozwijanego menu.</li><li>4. Zaakceptuj wartości domyślne lub zmień ustawienia w polach <b>Nazwa narzędzia przenoszenia danych</b>, <b>Nazwa hosta narzędzia przenoszenia danych</b>, <b>Użytkownik vCenter</b> i <b>Hasło vCenter</b>.</li><li>5. Kliknij opcję <b>Dodaj</b>, gdy ustawienia będą kompletne.</li></ol> <p>Więcej informacji na ten temat zawiera sekcja Konfigurowanie węzłów narzędzia przenoszenia danych z użyciem interfejsu GUI wtyczki vSphere w podręczniku instalowania interfejsu GUI programu Data Protection for VMware vSphere.</p> |

| Opcja                                                                                                                                                                                | Opis                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Konfigurowanie nowego narzędzia przenoszenia danych na potrzeby obsługi znaczników w systemie Windows lub Linux za pomocą interfejsu GUI programu Data Protection for VMware vSphere | <ol style="list-style-type: none"> <li>1. W systemie, w którym zainstalowano interfejs GUI programu Data Protection for VMware vSphere, uruchom ten interfejs GUI, otwierając przeglądarkę WWW i wprowadzając adres serwera WWW interfejsu GUI. Na przykład:<br/> https://&lt;adres_webGUI&gt;:<br/> 9081/TsmVMwareUI/</li> <li>2. Zaloguj się, używając ID użytkownika i hasła vCenter.</li> <li>3. Przejdź do karty <b>Konfiguracja</b> i wybierz działanie <b>Edytuj konfigurację programu IBM Spectrum Protect</b>.</li> <li>4. Przejdź do strony konfiguracji Węzły narzędzia przenoszenia danych.</li> <li>5. Dodaj węzeł narzędzia przenoszenia danych, wykonując następujące kroki: <ol style="list-style-type: none"> <li>a. Dla węzła narzędzia przenoszenia danych, dla którego chcesz skonfigurować obsługę znaczników, wybierz opcję <b>Utwórz usługi</b>. Domyślnie wybrana jest opcja <b>Węzeł obsługuje znaczniki</b> do włączenia węzła narzędzia przenoszenia danych do obsługi znaczników.</li> <li>b. Aby wyznaczyć węzeł obsługujący znaczniki jako węzeł domyślnego narzędzia przenoszenia danych, wybierz opcję <b>Domyślne narzędzie przenoszenia danych</b>. Węzeł domyślnego narzędzia przenoszenia danych tworzy kopie zapasowe wszystkich nowych maszyn wirtualnych dodawanych do dowolnego kontenera w centrum przetwarzania danych, jeśli kontener jest już w zestawie ochrony. Ponadto domyślne narzędzie przenoszenia danych tworzy kopie zapasowe maszyn wirtualnych w zestawie ochrony bez przypisanego znacznika <b>Narzędzie przenoszenia danych</b>.<br/> <b>Wskazówka:</b> W przypadku systemów Linux, po wybraniu nowego węzła narzędzia przenoszenia danych jako domyślnego węzła znaczników, należy następnie usunąć wiersz <b>vmtagdefaultdatamover</b> z każdego innego pliku opcji narzędzia przenoszenia danych, które jest powiązane z tym centrum przetwarzania danych.</li> <li>c. Kliknij przycisk <b>OK</b>, aby zapisać zmiany. Opcje <b>vmtagdatamover</b> i <b>vmtagdefaultdatamover</b>, jeśli są ustawione, są dodawane do pliku opcji narzędzia przenoszenia danych (<b>dsm.opt</b>).</li> </ol> </li> </ol> |

| Opcja                                                                                                                                                                                                                                                                                                      | Opis                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Konfigurowanie <i>istniejącego</i> węzła narzędzia przenoszenia danych w systemie Windows na potrzeby obsługi znaczników, gdy węzeł ten znajduje się na tym samym serwerze co interfejs GUI programu Data Protection for VMware vSphere                                                                    | <ol style="list-style-type: none"> <li>Wykonaj kroki od 1 do 3 z poprzedniej instrukcji w celu skonfigurowania nowego węzła narzędzia przenoszenia danych na potrzeby obsługi znaczników.</li> <li>Na stronie Węzły narzędzia przenoszenia danych wybierz opcję <b>Węzeł obsługuje znaczniki</b> dla węzła, dla którego chcesz włączyć obsługę znaczników.</li> <li><b>Opcjonalnie:</b> Aby wyznaczyć węzeł obsługujący znaczniki jako węzeł domyślnego narzędzia przenoszenia danych, wybierz opcję <b>Domyślne narzędzie przenoszenia danych</b>.</li> </ol>                                                                                                                                                                                                                                  |
| Konfigurowanie <i>istniejącego</i> węzła narzędzia przenoszenia danych w systemie Linux na potrzeby obsługi znaczników lub istniejącego węzła narzędzia przenoszenia danych w systemie Windows, gdy węzeł ten znajduje się na serwerze innym niż interfejs GUI programu Data Protection for VMware vSphere | <ol style="list-style-type: none"> <li>Dodaj opcję vmtagdatamover yes w pliku opcji narzędzia przenoszenia danych (dsm.sys w systemie Linux i dsm.opt w systemie Windows).</li> <li><b>Opcjonalnie:</b> Aby wyznaczyć węzeł obsługujący znaczniki jako węzeł domyślnego narzędzia przenoszenia danych, dodaj opcję vmtagdefaultdatamover yes lub vmtagdefaultdatamover <i>nazwa_narzędzia_przenoszenia_danych</i> do pliku opcji narzędzia przenoszenia danych.<br/><b>Wskazówka:</b> W przypadku systemów Linux, po wybraniu nowego węzła narzędzia przenoszenia danych jako domyślnego węzła znaczników, należy następnie usunąć wiersz vmtagdefaultdatamover z każdego innego pliku opcji narzędzia przenoszenia danych, które jest powiązane z tym centrum przetwarzania danych.</li> </ol> |

## Wyniki

Gdy dla węzła narzędzia przenoszenia danych włączono obsługę znaczników, narzędzie przenoszenia danych wysyła zapytania do spisu zasobów VMware w celu uzyskania informacji o znacznikach podczas operacji tworzenia kopii zapasowej. Następnie narzędzie przenoszenia danych tworzy kopię zapasową maszyn wirtualnych zgodnie z ustawionymi znacznikami ochrony danych. Jeśli węzeł narzędzia przenoszenia danych nie jest skonfigurowany do obsługi znaczników, znaczniki ochrony danych są ignorowane podczas operacji tworzenia kopii zapasowej.

### Informacje pokrewne:

➞ Vmtagdatamover

➞ Vmtagdefaultdatamover

➞ Konfigurowanie strategii tworzenia kopii zapasowych

---

# Konfigurowanie środowiska dla operacji natychmiastowego odtwarzania pełnej maszyny wirtualnej

Skonfiguruj dedykowaną sieć iSCSI dla operacji natychmiastowego odtwarzania pełnej maszyny wirtualnej i operacji natychmiastowego dostępu.

## Zanim rozpoczniesz

Należy użyć odpowiedniej dokumentacji środowiska VMware (ESXi lub vSphere), aby określić konkretne kroki, które należy wykonać w celu skonfigurowania wirtualnego przełącznika iSCSI i sieci maszyny wirtualnej. Chociaż podano ogólne wytyczne, właściwa dokumentacja i konkretne wyjaśnienia dotyczące sposobu dodawania sieci wirtualnych i przełączników wirtualnych przekraczają zakres dokumentacji tego produktu. W chwili publikacji dokumentacja produktów VMware vSphere ESXi i vCenter 5.5 była dostępna w następującym miejscu: dokumentacja środowiska VMware ESXi i serwera vCenter w wersji 5. Tematy „Networking” zawierają informacje dotyczące dodawania i konfigurowania przełączników wirtualnych i sieci wirtualnych.

**Ważne:** Te ustawienia konfiguracyjne udostępniono, aby ułatwić użytkownikowi skonfigurowanie środowiska VMware na potrzeby wykonywania efektywnych operacji natychmiastowego odtwarzania pełnych maszyn wirtualnych i natychmiastowego dostępu do tych maszyn. Jednak ze względu na to, że ustawienia te dotyczą czynności konfiguracyjnych środowiska VMware i interfejsów użytkownika środowiska VMware, należy zapoznać się z odpowiednią dokumentacją środowiska VMware, aby uzyskać szczegółowe instrukcje zawierające poszczególne kroki.

## O tym zadaniu

Ta procedura wymaga adaptera iSCSI na każdym hoście ESXi, który jest używany dla operacji natychmiastowego odtwarzania. Należy użyć odpowiedniej dokumentacji środowiska VMware, aby skonfigurować adapter. W momencie publikacji następujące procedury będą dostępne w tym zasobie VMware vSphere.

- Aby skonfigurować programowy adapter iSCSI, należy wykonać instrukcje zawarte w procedurze VMware „Configure Software iSCSI Adapters”.
- Aby skonfigurować sprzętowy adapter iSCSI, należy wykonać instrukcje zawarte w procedurze VMware „Setting Up Independent Hardware iSCSI Adapters”.

## 1. Konfigurowanie oprogramowania iSCSI na hoście ESXi

### Procedura

W ramach tego zadania oprogramowanie iSCSI jest konfigurowane na potrzeby konfiguracji podstawowej.

1. Zaloguj się do hosta ESXi, który ma być używany dla operacji natychmiastowego odtwarzania.
2. Wykonaj instrukcje podane w tym artykule bazy wiedzy środowiska VMware, aż zostanie włączony adapter iSCSI: <http://kb.vmware.com/kb/1008083>  
Program IBM Spectrum Protect automatycznie wykryje docelowy serwer iSCSI.
3. Upewnij się, że adres IP adaptera iSCSI (na hoście ESXi) ma ten sam adres podsieci, który jest używany przez narzędzie przenoszenia danych.
4. Upewnij się, że licencja na komponent Storage vMotion jest włączona na tym hoście ESXi.

## Co dalej

Gdy oprogramowanie iSCSI na hoście ESXi zostanie skonfigurowane, należy zainstalować i skonfigurować aplikacje w systemie narzędzia przenoszenia danych.

## 2. Instalowanie i konfigurowanie aplikacji w narzędziu przenoszenia danych

### Zanim rozpocznie

Jeśli agent odtwarzania i narzędzie przenoszenia danych programu IBM Spectrum Protect są już zainstalowane i skonfigurowane w systemie narzędzia przenoszenia danych, należy rozpocząć wykonywanie czynności od kroku 3.

### Procedura

W ramach tego zadania konfigurowany jest system narzędzia przenoszenia danych z aplikacjami i ustawieniami dla operacji natychmiastowego odtwarzania.

1. Zainstaluj agenta odtwarzania i narzędzie przenoszenia danych programu IBM Spectrum Protect w systemie narzędzia przenoszenia danych.

W kroku 4 procedury Instalowanie programu Data Protection for VMware wybierz typ instalacji **Zainstaluj pełny węzeł przenoszenia danych w celu ochrony aplikacji działających w systemie gościa**.

2. Skonfiguruj narzędzie przenoszenia danych.  
Postępuj zgodnie z instrukcjami podanymi w temacie Konfigurowanie narzędzia przenoszenia danych w dokumentacji klienta.

3. Ustaw adres IP serwera iSCSI:

- a. Przejdź do pliku C:\Program Files\Tivoli\TSM\baclient\dsm.opt i podaj następujące parametry:

VMISCSIServeraddress=<adres IP karty sieciowej w systemie narzędzia przenoszenia danych, który udostępnia obiekty docelowe iSCSI.>

Jeśli w systemie narzędzia przenoszenia danych znajduje się więcej niż jedna karta sieciowa, sprawdź, czy podano poprawną kartę sieciową dla sieci iSCSI.

## Co dalej

Po skonfigurowaniu systemu narzędzia przenoszenia danych należy nawiązać połączenie między interfejsem CLI agenta odtwarzania i interfejsem GUI agenta odtwarzania.

## 3. Konfigurowanie połączenia agenta odtwarzania

### Zanim rozpocznie

Interfejs wiersza komend (CLI) agenta odtwarzania w wersji 7.1.x można traktować jako interfejs API wiersza komend do interfejsu GUI agenta odtwarzania. Interfejsu CLI agenta odtwarzania można używać do komunikacji z interfejsem GUI agenta odtwarzania.

### Procedura

W ramach tego zadania nawiązywane jest połączenie między interfejsem CLI agenta odtwarzania i interfejsem GUI agenta odtwarzania.

1. Uruchom interfejs CLI agenta odtwarzania w systemie narzędzia przenoszenia danych.  
W menu **Start** systemu Windows kliknij kolejno opcje **Programy > IBM Spectrum Protect > IBM Spectrum Protect for Virtual Environments > IBM Spectrum Protect Recovery Agent**.



2. W oknie wiersza komend wprowadź następującą komendę:  
`RecoveryAgentShell.exe -c set_connection mount_computer <adres IP karty sieciowej w systemie narzędzia przenoszenia danych, który udostępnia obiekty docelowe iSCSI.>`

Ta komenda powoduje nawiązanie połączenia między interfejsem CLI agenta odtwarzania i interfejsem GUI agenta odtwarzania.

## Co dalej

Po nawiązaniu połączenia należy skonfigurować dedykowaną sieć iSCSI.

## 4. Konfigurowanie dedykowanej sieci iSCSI dla hosta ESXi i narzędzia przenoszenia danych

### Zanim rozpocznie

Przed wykonaniem tego zadania należy się zapoznać z następującymi wytycznymi:

- Dla operacji natychmiastowego odtwarzania należy używać dedykowanej sieci iSCSI.
- Każdy host ESXi, który jest używany dla operacji natychmiastowego odtwarzania, musi mieć dostępną drugą fizyczną kartę sieciową. Ta druga karta sieciowa jest powiązana z programowym adapterem iSCSI odpowiedniego hosta ESXi.
- Dla systemu narzędzia przenoszenia danych działającego w maszynie wirtualnej musi być dostępna druga karta sieciowa. Ta druga karta sieciowa jest powiązana z programowym adapterem iSCSI hosta ESXi.
- Każdy host ESXi, który jest używany dla operacji natychmiastowego odtwarzania, musi mieć dostępną drugą składnicę danych VMware. Ta tymczasowa składnica danych zawiera informacje konfiguracyjne i dane maszyny wirtualnej tworzonej podczas tej operacji.

## Procedura

W ramach tego zadania konfigurowana jest dedykowana sieć iSCSI dla hosta ESXi i dla narzędzia przenoszenia danych działającego w maszynie wirtualnej.

1. Zaloguj się do hosta ESXi, który ma być używany dla operacji natychmiastowego odtwarzania.
2. Skonfiguruj przełącznik wirtualny dla sieci iSCSI.  
W podanych krokach przełącznikiem wirtualnym jest *vSwitch1*.
  - a. Wybierz opcję **VMkernel Network Adapter** (Adapter sieciowy VMkernel) jako **Connection Type** (Typ połączenia).  
Ten typ połączenia jest wymagany przez sieć iSCSI.
  - b. Wybierz opcję **Create a vSphere standard switch** (Utwórz standardowy przełącznik vSphere) dla parametru **VMkernel Network Access** (Dostęp do sieci VMkernel).
  - c. Wybierz opcję **Network Label** (Etykieta sieci) dla parametru **VMkernel Connection Settings** (Ustawienia połączenia VMkernel).  
Podaj etykietę wskazującą *vSwitch1* i tę sieć dla ruchu danych iSCSI.  
Na przykład: *VMkernel iSCSI*.
  - d. Podaj adres IP i maskę podsieci dla *vSwitch1* w parametrze **VMkernel IP Connection Settings** (Ustawienia połączenia IP VMkernel).  
Nie zmieniaj wartości parametrów **Subnet Mask** (Maska podsieci) ani **VMkernel Default Gateway** (Domyślna brama VMkernel).
  - e. Podaj port jądra na potrzeby działania sieci iSCSI.
3. Skonfiguruj przełącznik wirtualny dla sieci maszyny wirtualnej.  
W podanych krokach przełącznikiem wirtualnym jest *vSwitch0*.

- a. Wybierz opcję **Virtual Machine** (Maszyna wirtualna) jako **Connection Type** (Typ połączenia).
  - b. Wybierz opcję **Create a vSphere standard switch** (Utwórz standardowy przełącznik vSphere) dla parametru **VMkernel Network Access** (Dostęp do sieci VMkernel).
  - c. Przejdź do karty **Port Group Properties** (Właściwości grupy portów) i wybierz opcję **Network Label** (Etykieta sieci).  
Podaj taką samą etykietę, która została podana dla sieci maszyny wirtualnej *vSwitch1*.  
Na przykład: *VMkernel iSCSI*.
4. Powiąż nowo utworzony adapter iSCSI z adapterem **VMkernel Network Adapter** (Adapter sieciowy VMkernel).  
Wykonaj instrukcje podane w procedurze VMware „Bind iSCSI Adapters with VMkernel Adapters”. W chwili publikacji ta procedura była dostępna w dokumentacji środowiska VMware ESXi i serwera vCenter w wersji 5.
- Wskazówka:** Jeśli podczas skanowania urządzeń iSCSI zostanie przekroczony limit czasu, należy zmniejszyć liczbę urządzeń iSCSI podłączonych do hosta ESXi. Następnie należy ponownie wykonać skanowanie urządzeń iSCSI.
5. Upewnij się, że właściwości powiązania adaptera iSCSI są poprawne.
- a. Przejdź do opcji **Hardware (Sprzęt) > Storage Adapters (Adaptory pamięci masowej)** w kliencie VMware vSphere.
  - b. Prawym przyciskiem myszy kliknij adapter iSCSI i wybierz opcję **iSCSI Initiator Properties** (Właściwości inicjatora iSCSI). Upewnij się, że istnieją następujące właściwości powiązania:

Tabela 10. Ustawienia sieci iSCSI

| Sieć maszyny wirtualnej                              | Sieć iSCSI                                                                                                                                                                                                                   |
|------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Standard Switch:</b> <i>vSwitch0</i>              | <b>Standard Switch:</b> <i>vSwitch1</i>                                                                                                                                                                                      |
| <b>Virtual Machine Port Group:</b> <i>VM Network</i> | <b>VMkernel Port:</b> <i>VMkernel iSCSI</i><br><b>Wskazówka:</b> <i>VMkernel iSCSI</i> jest przypisane do<br><b>VMkernel Adapter:</b> <i>vmk1</i> , który znajduje się w<br><b>Physical Network Adapter:</b> <i>vmnic1</i> . |
| <b>Physical Adapter:</b> <i>vmnic0</i>               | <b>VMkernel Network Adapter:</b> <i>vmk1</i>                                                                                                                                                                                 |
|                                                      | <b>Physical Network Adapter:</b> <i>vmnic1</i>                                                                                                                                                                               |
|                                                      | <b>Virtual Network Adapter IP address:</b><br>192.168.42.x (podsieć dla sieci iSCSI)                                                                                                                                         |

## Wyniki

Dedykowana sieć iSCSI jest gotowa dla operacji natychmiastowego odtwarzania pełnej maszyny wirtualnej i operacji natychmiastowego dostępu.

## Konfigurowanie ustawień zabezpieczeń dla produktu Data Protection for VMware

Narzędzia przenoszenia danych produktu Data Protection for VMware, interfejs wiersza komend *vmcli* i komponenty interfejsu GUI programu Data Protection for VMware vSphere wymagają skonfigurowania, aby umożliwić bezpieczne połączenie z serwerem IBM Spectrum Protect.

## Konfigurowanie ustawień zabezpieczeń w celu połączenia narzędzia przenoszenia danych i węzłów VMCLI z serwerem IBM Spectrum Protect

Istnieje szereg opcji konfiguracyjnych, które odnoszą się do ustawień zabezpieczeń produktu Data Protection for VMware dla narzędzia przenoszenia danych i węzłów VMCLI podczas nawiązywania połączenia z serwerem IBM Spectrum Protect w wersji 7.1.8, 8.1.2 lub nowszej. Zaakceptowanie wartości domyślnych dla tych opcji powoduje niezauważalne skonfigurowanie tych komponentów w celu zwiększenia bezpieczeństwa i jest zalecane w większości przypadków użycia.

### Konfigurowanie z użyciem domyślnych ustawień zabezpieczeń (krótka ścieżka)

Krótka ścieżka wskazuje opcje konfiguracyjne, które mają wpływ na bezpieczeństwo połączenia narzędzia przenoszenia danych i węzła VMCLI z serwerem, a także różne przypadki użycia, gdy zostaną zaakceptowane wartości domyślne. W scenariuszu z użyciem krótkiej ścieżki minimalizowana jest liczba kroków w procesie konfigurowania punktów końcowych.

W tym scenariuszu certyfikaty są automatycznie uzyskiwane z serwera, gdy węzeł łączy się po raz pierwszy, przy założeniu, że parametr **SESSIONSECURITY** serwera IBM Spectrum Protect jest ustawiony na wartość **TRANSITIONAL** (jest to wartość domyślna przy pierwszym połączeniu). Ten scenariusz można wykonać, gdy najpierw wykonywana jest aktualizacja serwera IBM Spectrum Protect do wersji 7.1.8 i nowszych wersji 7 lub do wersji 8.1.2 i nowszych wersji 8, a następnie wykonywana jest aktualizacja produktu Data Protection for VMware do tych wersji (lub odwrotnie).

**Ważne:** Nie można użyć tego scenariusza, jeśli serwer IBM Spectrum Protect jest skonfigurowany do uwierzytelniania LDAP. Jeśli używany jest protokół LDAP, można ręcznie zaimportować niezbędne certyfikaty za pomocą programu narzędziowego dsmscert. Więcej informacji na ten temat zawiera sekcja “Konfigurowanie bez automatycznej dystrybucji certyfikatów” na stronie 60.

### Opcje węzła narzędzia przenoszenia danych mające wpływ na bezpieczeństwo sesji

Następujące opcje dsmsc określają ustawienia zabezpieczeń dla węzła narzędzia przenoszenia danych. Więcej informacji na temat tych opcji zawiera sekcja Skorowidz opcji klienta.

- **SSLREQUIRED.** Wartość domyślna **Default** obsługuje istniejące połączenia z bezpieczeństwem sesji z serwerami w wersjach wcześniejszych niż 7.1.8 lub 8.1.2 i automatycznie konfiguruje narzędzie przenoszenia danych programu Data Protection for VMware na potrzeby bezpiecznego łączenia się z serwerami w wersji 7.1.8 lub 8.1.2 albo w nowszej wersji przy użyciu uwierzytelniania za pomocą protokołu TLS.
- **SSLACCEPTCERTFROMSERV.** Wartość domyślna **Yes** powoduje, że narzędzie przenoszenia danych automatycznie akceptuje samopodpisany certyfikat publiczny z serwera i automatycznie konfiguruje narzędzie przenoszenia danych do korzystania z tego certyfikatu, gdy łączy się ono z serwerem w wersji 7.1.8 lub 8.1.2 albo nowszej.
- **SSL.** Wartość domyślna **No** wskazuje, że szyfrowanie nie jest używane przy przesyłaniu danych między narzędziem przenoszenia danych i serwerem w wersji wcześniejszej niż 7.1.8 lub 8.1.2. Gdy narzędzie przenoszenia danych łączy się z serwerem w wersji 7.1.8 lub 8.1.2 albo nowszej, wartość domyślna **No** wskazuje, że dane obiektów nie są szyfrowane. Wszystkie pozostałe informacje są szyfrowane, gdy narzędzie przenoszenia danych komunikuje się z serwerem. Wartość **Yes** wskazuje, że protokół TLS jest używany do szyfrowania wszystkich informacji, w tym danych obiektów, gdy narzędzie przenoszenia danych komunikuje się z serwerem.

- **SSLFIPSMODE.** Wartość domyślna **No** wskazuje, że biblioteka TLS z certyfikatem FIPS (Federal Information Processing Standards) nie jest wymagana.

Dodatkowo następujące opcje mają zastosowanie tylko wtedy, gdy narzędzie przenoszenia danych używa połączenia TLS z serwerem w wersji wcześniejszej niż 7.1.8 lub 8.1.2. Są one ignorowane, gdy narzędzie przenoszenia danych łączy się z serwerem w nowszej wersji.

- **SSLDISABLELEGACYTLS.** Wartość **No** wskazuje, że narzędzie przenoszenia danych nie wymaga protokołu TLS 1.2 dla sesji SSL. Umożliwia ona połączenie z użyciem protokołu TLS 1.1 i starszych protokołów SSL. Gdy narzędzie przenoszenia danych komunikuje się z serwerem IBM Spectrum Protect w wersji 7.1.7 lub 8.1.1 albo wcześniejszej, **No** jest wartością domyślną.
- **LANFREESL.** Wartość domyślna **No** wskazuje, że narzędzie przenoszenia danych nie używa protokołu TLS podczas komunikacji z agentem pamięci masowej, gdy skonfigurowano przesyłanie danych bez obciążania sieci LAN.
- **REPLSSLPORT.** Określa adres portu protokołu TCP/IP, który jest włączony dla protokołu TLS, gdy narzędzie przenoszenia danych komunikuje się z docelowym serwerem replikacji.

## Opcje węzła VMCLI mające wpływ na bezpieczeństwo sesji

Następujące parametry określają ustawienia zabezpieczeń dla węzła VMCLI. Więcej informacji na temat tych opcji zawiera sekcja Parametry profilu.

- **VE\_TSM\_SSL.** Wartość domyślna **NO** wskazuje, że szyfrowanie nie jest używane przy przesyłaniu danych między narzędziem przenoszenia danych i serwerem w wersji wcześniejszej niż 7.1.8 lub 8.1.2. Należy ustawić wartość **YES**, jeśli protokół TLS ma być używany do szyfrowania wszystkich informacji podczas łączenia się z serwerem w wersji starszej niż 7.1.8.
- **VE\_TSM\_SSLACCEPTCERTFROMSERV.** Wartość domyślna **YES** powoduje, że interfejs automatycznie akceptuje samopodpisany certyfikat publiczny z serwera i automatycznie konfiguruje interfejs do korzystania z tego certyfikatu, gdy łączy się on z serwerem w wersji 7.1.8 lub 8.1.2 albo nowszej.
- **VE\_TSM\_SSLREQUIRED.** Wartość domyślna **DEFAULT** obsługuje istniejące połączenia z bezpieczeństwem sesji z serwerami w wersjach wcześniejszych niż 7.1.8 lub 8.1.2 i automatycznie konfiguruje interfejs na potrzeby bezpiecznego łączenia się z serwerami w wersji 7.1.8 lub 8.1.2 albo w nowszej wersji przy użyciu uwierzytelniania za pomocą protokołu TLS.

## Przypadki użycia dla domyślnych ustawień zabezpieczeń

- Najpierw serwer jest aktualizowany do wersji 7.1.8, 8.1.2 lub nowszej. Następnie aktualizowany jest produkt Data Protection for VMware. Istniejące narzędzie przenoszenia danych i węzły VMCLI *nie korzystają* z komunikacji SSL:
  - Nie są wymagane żadne zmiany w opcjach zabezpieczeń dla narzędzia przenoszenia danych i węzłów VMCLI.
  - Konfiguracja jest automatycznie aktualizowana do używania protokołu TLS, gdy węzły uwierzytelniają się na serwerze.
- Najpierw serwer jest aktualizowany do wersji 7.1.8, 8.1.2 lub nowszej. Następnie aktualizowany jest produkt Data Protection for VMware. Istniejące narzędzie przenoszenia danych i węzły VMCLI *korzystają* z komunikacji SSL:
  - Nie są wymagane żadne zmiany w opcjach zabezpieczeń dla narzędzia przenoszenia danych i węzłów VMCLI.
  - Komunikacja SSL z użyciem istniejącego certyfikatu publicznego serwera jest nadal używana.

- Komunikacja SSL jest automatycznie rozszerzana do korzystania z poziomu TLS wymaganego przez serwer.
- Najpierw produkt Data Protection for VMware jest aktualizowany do wersji 7.1.8, 8.1.2 lub nowszej. Następnie aktualizowany jest serwer (w późniejszym czasie). Istniejące narzędzie przenoszenia danych i węzły VMCLI *nie korzystają* z komunikacji SSL:
  - Nie są wymagane żadne zmiany w opcjach zabezpieczeń dla narzędzia przenoszenia danych i węzłów VMCLI.
  - Istniejący protokół uwierzytelniania jest nadal używany dla serwerów w wersjach starszych niż 7.1.8 lub 8.1.2.
  - Konfiguracja jest automatycznie aktualizowana do używania protokołu TLS, gdy węzły uwierzytelniają się na serwerze po zaktualizowaniu serwera do wersji 7.1.8 lub 8.1.2 albo nowszej.
- Najpierw produkt Data Protection for VMware jest aktualizowany do wersji 7.1.8, 8.1.2 lub nowszej. Następnie aktualizowany jest serwer (w późniejszym czasie). Istniejące narzędzie przenoszenia danych i węzły VMCLI *korzystają* z komunikacji SSL:
  - Nie są wymagane żadne zmiany w opcjach zabezpieczeń dla narzędzia przenoszenia danych i węzłów VMCLI.
  - Komunikacja SSL z użyciem istniejącego certyfikatu publicznego serwera jest nadal używana dla serwerów w wersji starszej niż 7.1.8 lub 8.1.2.
  - Komunikacja SSL jest automatycznie rozszerzana do korzystania z poziomu TLS wymaganego przez serwer po zaktualizowaniu serwera do wersji 7.1.8 lub 8.1.2 albo nowszej.
- Najpierw produkt Data Protection for VMware jest aktualizowany do wersji 7.1.8, 8.1.2 lub nowszej. Następnie narzędzie przenoszenia danych i węzły VMCLI łączą się z wieloma serwerami. Serwery są aktualizowane w różnych momentach:
  - Nie są wymagane żadne zmiany w opcjach zabezpieczeń dla narzędzia przenoszenia danych i węzłów VMCLI.
  - Narzędzie przenoszenia danych i węzły VMCLI używają istniejącego protokołu uwierzytelniania i bezpieczeństwa sesji dla serwerów w wersjach starszych niż 7.1.8 lub 8.1.2 i automatycznie przeprowadzają aktualizację w celu użycia uwierzytelniania TLS przy początkowym połączeniu się z serwerem w wersji 7.1.8 lub 8.1.2 albo nowszej. Bezpieczeństwem sesji zarządza serwer.
- Instalacja nowego klienta; serwer jest w wersji 7.1.8 lub 8.1.2 lub nowszej:
  - Skonfiguruj produkt Data Protection for VMware stosownie do nowej instalacji.
  - Wartości domyślne dla opcji zabezpieczeń automatycznie konfiguruje narzędzie przenoszenia danych i węzły VMCLI na potrzeby uwierzytelniania sesji szyfrowanej za pomocą protokołu TLS.
  - Dla parametru SSL ustaw wartość **Yes**, jeśli wymagane jest szyfrowanie wszystkich danych przesyłanych między klientem i serwerem.
- Instalacja nowego klienta; serwer jest w wersji starszej niż 7.1.8 lub 8.1.2:
  - Skonfiguruj klienta stosownie do instalacji nowego klienta.
  - Zaakceptuj wartości domyślne dla parametrów dotyczących bezpieczeństwa sesji, jeśli nie jest wymagane szyfrowanie wszystkich przesyłanych danych.
    - Do czasu zaktualizowania serwera do wersji 7.1.8 lub 8.1.2 albo nowszej używany jest protokół uwierzytelniania inny niż SSL.
  - Dla parametru SSL ustaw wartość **Yes**, jeśli wymagane jest szyfrowanie wszystkich danych przesyłanych między narzędziem przenoszenia danych i serwerem, a następnie kontynuuj ręczne konfigurowanie protokołu SSL.
    - Instrukcje dotyczące konfigurowania znajdują się w sekcji Konfigurowanie komunikacji klient/serwer programu Tivoli Storage Manager z użyciem protokołu Secure Sockets Layer.

- Komunikacja SSL jest automatycznie rozszerzana do korzystania z poziomu TLS wymaganego przez serwer po zaktualizowaniu serwera do wersji 7.1.8 lub 8.1.2 albo nowszej.

## Konfigurowanie bez automatycznej dystrybucji certyfikatów

W tym scenariuszu wskazano opcje konfiguracyjne, które mają wpływ na bezpieczeństwo narzędzia przenoszenia danych i węzłów VMCLI, gdy automatyczna dystrybucja certyfikatów z serwera nie jest dopuszczalna. Na przykład automatyczna dystrybucja certyfikatów z serwera nie jest dopuszczalna, jeśli serwer jest skonfigurowany do korzystania z uwierzytelniania LDAP lub konieczne jest, aby certyfikaty były podpisane przez ośrodek certyfikacji (CA).

## Opcje mające wpływ na bezpieczeństwo sesji

Opcje ustawień zabezpieczeń są takie same jak te, które są opisane w sekcji “Konfigurowanie z użyciem domyślnych ustawień zabezpieczeń (krótka ścieżka)” na stronie 57, z tym wyjątkiem, że dla opcji `SSLACCEPTCERTFROMSERV` należy ustawić wartość `No`, aby węzeł narzędzia przenoszenia danych automatycznie nie akceptował samopodpisanego certyfikatu publicznego z serwera, gdy węzeł ten po raz pierwszy łączy się z serwerem w wersji 7.1.8 lub 8.1.2 albo nowszej.

## Przypadki użycia dla konfigurowania węzłów narzędzia przenoszenia danych bez automatycznej dystrybucji certyfikatów

Jeśli automatyczna dystrybucja certyfikatów jest niemożliwa lub niepożądana, należy użyć programu narzędziowego `dsmcert` do zaimportowania certyfikatu. Należy uzyskać niezbędny certyfikat z serwera IBM Spectrum Protect lub z ośrodka CA. Certyfikat od ośrodka CA może pochodzić z firmy, takiej jak VeriSign lub Thawte, ale może też pochodzić od wewnętrznego ośrodka CA firmy.

Jeśli narzędzie przenoszenia danych i węzły VMCLI znajdują się na tym samym komputerze, wymagany jest tylko jeden certyfikat. Jeśli węzły znajdują się na różnych komputerach, wymagany jest jeden certyfikat dla każdego komputera.

- Najpierw serwer jest aktualizowany do wersji 7.1.8 lub 8.1.2. Następnie aktualizowany jest produkt Data Protection for VMware. Istniejące węzły narzędzia przenoszenia danych *nie korzystają* z komunikacji SSL:
  - Dla opcji `SSLACCEPTCERTFROMSERV` ustaw wartość `No`.
  - Uzyskaj niezbędny certyfikat z serwera IBM Spectrum Protect lub z ośrodka CA, a następnie użyj programu narzędziowego `dsmcert` do zaimportowania tego certyfikatu. Instrukcje dotyczące konfigurowania znajdują się w sekcji Konfigurowanie komunikacji klient/serwer programu Tivoli Storage Manager z użyciem protokołu Secure Sockets Layer.
- Najpierw serwer jest aktualizowany do wersji 7.1.8 lub 8.1.2. Następnie aktualizowany jest produkt Data Protection for VMware. Istniejące węzły narzędzia przenoszenia danych *korzystają* z komunikacji SSL:
  - Nie są wymagane żadne zmiany w opcjach zabezpieczeń dla węzłów narzędzia przenoszenia danych. Jeśli węzły mają już certyfikat serwera dla komunikacji SSL, opcja `SSLACCEPTCERTFROMSERV` nie ma zastosowania.
  - Komunikacja SSL z użyciem istniejącego certyfikatu publicznego serwera jest nadal używana.
  - Komunikacja SSL jest automatycznie rozszerzana do korzystania z poziomu TLS wymaganego przez serwer.

- Najpierw produkt Data Protection for VMware jest aktualizowany do wersji 7.1.8 lub 8.1.2. Następnie aktualizowany jest serwer (w późniejszym czasie). Istniejące węzły narzędzia przenoszenia danych *nie korzystają* z komunikacji SSL:
  - Dla opcji `SSLACCEPTCERTFROMSERV` ustaw wartość `No`.
  - Istniejący protokół uwierzytelniania jest nadal używany dla serwerów w wersjach starszych niż 7.1.8 lub 8.1.2.
  - Zanim węzły narzędzia przenoszenia danych połączą się z serwerem w wersji 7.1.8 lub 8.1.2 albo nowszej:
    - Uzyskaj niezbędny certyfikat z serwera IBM Spectrum Protect lub z ośrodka CA, a następnie użyj programu narzędziowego `dsmcert` do zaimportowania tego certyfikatu. Instrukcje dotyczące konfigurowania znajdują się w sekcji Konfigurowanie komunikacji klient/serwer programu Tivoli Storage Manager z użyciem protokołu Secure Sockets Layer.
- Najpierw produkt Data Protection for VMware jest aktualizowany do wersji 7.1.8 lub 8.1.2. Następnie aktualizowany jest serwer (w późniejszym czasie). Istniejące węzły narzędzia przenoszenia danych *korzystają* z komunikacji SSL.
  - Nie są wymagane żadne zmiany w opcjach zabezpieczeń dla węzłów narzędzia przenoszenia danych. Jeśli węzły mają już certyfikat serwera dla komunikacji SSL, opcja `SSLACCEPTCERTFROMSERV` nie ma zastosowania.
  - Komunikacja SSL z użyciem istniejącego certyfikatu publicznego serwera jest nadal używana dla serwerów w wersji starszej niż 7.1.8 lub 8.1.2.
  - Komunikacja SSL jest automatycznie rozszerzana do korzystania z poziomu TLS wymaganego przez serwer po zaktualizowaniu serwera do wersji 7.1.8 lub 8.1.2 albo nowszej.
- Najpierw produkt Data Protection for VMware jest aktualizowany do wersji 7.1.8 lub 8.1.2. Następnie węzły narzędzia przenoszenia danych łączą się z wieloma serwerami. Serwery są aktualizowane w różnych momentach:
  - Dla opcji `SSLACCEPTCERTFROMSERV` ustaw wartość `No`.
  - Istniejący protokół uwierzytelniania jest nadal używany dla serwerów w wersjach starszych niż 7.1.8 lub 8.1.2.
  - Zanim węzły narzędzia przenoszenia danych połączą się z serwerem w wersji 7.1.8 lub 8.1.2 albo nowszej lub gdy komunikacja SSL jest wymagana na każdym poziomie serwera:
    - Uzyskaj niezbędny certyfikat z serwera IBM Spectrum Protect lub z ośrodka CA, a następnie użyj programu narzędziowego `dsmcert` do zaimportowania tego certyfikatu. Instrukcje dotyczące konfigurowania znajdują się w sekcji Konfigurowanie komunikacji klient/serwer programu Tivoli Storage Manager z użyciem protokołu Secure Sockets Layer.
  - Węzły narzędzia przenoszenia danych używają istniejącego protokołu uwierzytelniania i bezpieczeństwa sesji dla serwerów w wersjach starszych niż 7.1.8 lub 8.1.2 i automatycznie przeprowadzają aktualizację w celu użycia uwierzytelniania TLS przy początkowym połączeniu się z serwerem w wersji 7.1.8 lub 8.1.2 albo nowszej. Bezpieczeństwem sesji zarządza serwer.
- Nowa instalacja produktu Data Protection for VMware; serwer jest w wersji 7.1.8 lub 8.1.2 lub nowszej:
  - Skonfiguruj produkt Data Protection for VMware stosownie do nowej instalacji.
  - Dla opcji `SSLACCEPTCERTFROMSERV` ustaw wartość `No`.
  - Uzyskaj niezbędny certyfikat z serwera IBM Spectrum Protect lub z ośrodka CA, a następnie użyj programu narzędziowego `dsmcert` do zaimportowania tego certyfikatu.

Instrukcje dotyczące konfigurowania znajdują się w sekcji Konfigurowanie komunikacji klient/serwer programu Tivoli Storage Manager z użyciem protokołu Secure Sockets Layer.

- Dla parametru SSL ustaw wartość **Yes**, jeśli wymagane jest szyfrowanie wszystkich danych przesyłanych między narzędziem przenoszenia danych i serwerem.
- Nowa instalacja produktu Data Protection for VMware; serwer jest w wersji starszej niż 7.1.8 lub 8.1.2; sesje szyfrowane za pomocą protokołu SSL *są* wymagane:
  - Skonfiguruj produkt Data Protection for VMware stosownie do nowej instalacji.
  - Dla parametru SSL ustaw wartość **Yes**.
  - Uzyskaj niezbędny certyfikat z serwera IBM Spectrum Protect lub z ośrodka CA, a następnie użyj programu narzędziowego dsmcert do zaimportowania tego certyfikatu. Instrukcje dotyczące konfigurowania znajdują się w sekcji Konfigurowanie komunikacji klient/serwer programu Tivoli Storage Manager z użyciem protokołu Secure Sockets Layer.
- Nowa instalacja produktu Data Protection for VMware; serwer jest w wersji starszej niż 7.1.8 lub 8.1.2; sesje szyfrowane za pomocą protokołu SSL *nie są* wymagane:
  - Skonfiguruj produkt Data Protection for VMware stosownie do nowej instalacji.
  - Dla opcji SSLACCEPTCERTFROMSERV ustaw wartość **No**.
    - Do czasu zaktualizowania serwera do wersji 7.1.8 lub 8.1.2 albo nowszej używany jest protokół uwierzytelniania inny niż SSL.
  - Zanim węzły narzędzia przenoszenia danych połączą się z serwerem w wersji 7.1.8 lub 8.1.2 albo nowszej:
    - Uzyskaj niezbędny certyfikat z serwera IBM Spectrum Protect lub z ośrodka CA, a następnie użyj programu narzędziowego dsmcert do zaimportowania tego certyfikatu. Instrukcje dotyczące konfigurowania znajdują się w sekcji Konfigurowanie komunikacji klient/serwer programu Tivoli Storage Manager z użyciem protokołu Secure Sockets Layer.

## Konfigurowanie komunikacji interfejsu GUI Data Protection for VMware vSphere z użyciem protokołu TLS

Interfejs GUI Data Protection for VMware vSphere używa protokołu Transport Layer Security (TLS) w celu zapewnienia bezpiecznej komunikacji z przeglądarkami WWW, serwerem VMware vCenter i opcjonalnie z serwerem IBM Spectrum Protect.

### O tym zadaniu

Na potrzeby komunikacji z przeglądarkami WWW i serwerem VMware vCenter protokół TLS jest zawsze włączony. Podczas instalowania programu Data Protection for VMware generowany jest samopodpisany certyfikat cyfrowy TLS, który jest następnie używany na potrzeby połączenia.

Na potrzeby komunikacji z przeglądarkami WWW można także użyć certyfikatu podpisanego przez ośrodek certyfikacji (CA). Data Protection for VMware — informacje na temat używania certyfikatu z ośrodka CA zawiera sekcja Używanie certyfikatu innej firmy dla sesji przeglądarki WWW.

Na potrzeby komunikacji z serwerem IBM Spectrum Protect użycie protokołu TLS zależy od wersji tego serwera.

### Jeśli używany jest serwer IBM Spectrum Protect w wersji 7.1.7, 8.1.1 lub nowszej

Użycie protokołu TLS na potrzeby komunikacji z serwerem jest opcjonalne. Można ręcznie włączyć komunikację interfejsu GUI Data Protection for VMware vSphere z serwerem za pomocą protokołu TLS, tworząc lub aktualizując magazyn zaufanych



certyfiatów i importując certyfiat, jak to opisano w sekcji “Włączanie bezpiecznej komunikacji z serwerem IBM Spectrum Protect”.

#### **Jeśli używany jest serwer IBM Spectrum Protect w wersji 7.1.8, 8.1.2 lub nowszej**

Użycie protokołu TLS jest wymagane. W większości przypadków magazyn zaufanych certyfiatów jest tworzony automatycznie przy pierwszym użyciu z wykorzystaniem domyślnych ustawień zabezpieczeń, które zostały opisane w sekcji “Konfigurowanie z użyciem domyślnych ustawień zabezpieczeń (krótka ścieżka)” na stronie 57. Jednak w niektórych przypadkach może być konieczne ręczne utworzenie magazynu zaufanych certyfiatów.

**Ważne:** W tym scenariuszu certyfiaty są automatycznie uzyskiwane wtedy, gdy interfejs GUI Data Protection for VMware vSphere komunikuje się z serwerem po raz pierwszy, przy założeniu, że parametr **SESSIONSECURITY** serwera IBM Spectrum Protect jest ustawiony na wartość **TRANSITIONAL** (jest to wartość domyślna przy pierwszym połączeniu). Gdy interfejs GUI połączy się z serwerem, dla parametru **SESSIONSECURITY** ustawiana jest wartość **STRICT**. Ponieważ interfejs GUI do połączenia się z serwerem używa identyfikatora administratora serwera, jeśli inna jednostka użyła tego identyfikatora do połączenia, w interfejsie GUI zostanie wyświetlony komunikat o błędzie podczas próby nawiązania połączenia z serwerem. Aby rozwiązać ten problem, dla parametru **SESSIONSECURITY** należy z powrotem ustawić wartość **TRANSITIONAL**.

### **Włączanie bezpiecznej komunikacji z serwerem IBM Spectrum Protect**

Jeśli używany jest serwer IBM Spectrum Protect w wersji 7.1.7 lub wcześniejszej albo w wersji 8.1.2 lub wcześniejszej, połączenie z tym serwerem za pomocą protokołu TLS jest opcjonalne. Aby umożliwić komunikację interfejsu GUI Data Protection for VMware vSphere z serwerem za pomocą tego protokołu, należy ją włączyć ręcznie.

#### **Zanim rozpocznieś**

Uzyskaj kopię certyfikatu od administratora serwera.

#### **O tym zadaniu**

Jeśli używany jest serwer w wersji 7.1.8 lub 8.1.2 lub nowszej, protokół TLS jest wymagany i magazyn zaufanych certyfiatów z tym certyfikatem jest tworzony automatycznie przy pierwszym użyciu z wykorzystaniem domyślnych ustawień zabezpieczeń, które zostały opisane w sekcji “Konfigurowanie z użyciem domyślnych ustawień zabezpieczeń (krótka ścieżka)” na stronie 57. Jednak w niektórych przypadkach może być konieczne ręczne utworzenie magazynu zaufanych certyfiatów i skonfigurowanie interfejsu GUI Data Protection for VMware vSphere zgodnie z opisem w tym temacie.

W poniższej procedurze używane jest narzędzie Java™ do zarządzania kluczami i certyfiatami: **keytool**.

W systemach operacyjnych Linux narzędzie znajduje się w katalogu `/opt/tivoli/tsm/tdpvmware/common/jre/jre/bin/`.

W systemach operacyjnych Microsoft Windows narzędzie znajduje się w katalogu `C:\Program Files\Common Files\Tivoli\TSM\jvm80516\jre\bin`.

Podczas uruchamiania komendy narzędzia **keytool** może być konieczne podanie pełnej ścieżki.

## Procedura

1. Z poziomu wiersza komend przejdź do katalogu magazynu zaufanych certyfikatów:
  - W systemie Linux: `/opt/tivoli/tsm/tdpvmware/common/scripts/`
  - W systemie Windows: `C:\Program Files\IBM\SpectrumProtect\Framework\VEGUI\scripts\`
2. Utwórz magazyn zaufanych certyfikatów i zaimportuj certyfikat za pomocą następującej komendy:  

```
keytool -importcert -alias certyfiakat -file cert.pem -keystore
tsm-ve-truststore.jks -storepass hasło
```

Gdzie:

  - alias *certyfiakat***  
Unikalny alias, który identyfikuje certyfikat w magazynie zaufanych certyfikatów.
  - file *cert.pem***  
Plik, który zawiera certyfikat samopodpisany serwera lub certyfikat główny ośrodka CA.
  - storepass *hasło***  
Hasło magazynu kluczy. Należy zapamiętać to hasło w celu użycia w przyszłości.
3. Uruchom interfejs GUI programu Data Protection for VMware vSphere i przejdź do okna Konfiguracja.
  - Jeśli tworzysz konfigurację początkową, kliknij opcję **Zadania > Uruchom kreatora konfiguracji IBM Spectrum Protect** i przejdź do strony Informacje autoryzacyjne serwera.
  - Jeśli modyfikujesz istniejącą konfigurację, kliknij opcję **Zadania > Edytuj konfigurację IBM Spectrum Protect** i przejdź do strony Informacje autoryzacyjne serwera.
4. W polu **Port administracyjny IBM Spectrum Protect** wpisz numer portu. Jest to port serwera, który zezwala na połączenia administracyjne przy użyciu protokołów SSL lub TLS.
5. Wybierz opcję **Użyj szyfrowanej komunikacji na porcie administracyjnym**.
6. Jeśli chcesz użyć tego ustawienia dla przyszłych sesji interfejsu GUI, wybierz opcję **Zapisz ID administratora, hasło i ustawienia portu**.
7. Kliknij przycisk **OK**, aby zastosować zmiany.

## Używanie certyfikatu z ośrodka certyfikacji

Aby użyć certyfikatu, który jest podpisany przez ośrodek certyfikacji (CA), należy wykonać wiele kroków.

### O tym zadaniu

W poniższych procedurach używane jest standardowe narzędzie do zarządzania kluczami i certyfikatami mające nazwę **keytool**.

W systemach operacyjnych Linux znajduje się ono w katalogu `/opt/tivoli/tsm/tdpvmware/common/jre/jre/bin/`.

W systemach operacyjnych Microsoft Windows narzędzie to znajduje się w katalogu `C:\Program Files\Common Files\Tivoli\TSM\jvm80516\jre`.

Podczas uruchamiania narzędzia **keytool** za pomocą wiersza komend może być konieczne podanie pełnej ścieżki.

### Procedura

1. Uzyskaj dostęp do magazynu kluczy.
2. Utwórz żądanie podpisania certyfikatu (CSR).
3. Wyślij żądanie podpisania certyfikatu do ośrodka certyfikacji w celu podpisania certyfikatu.
4. Pobierz podpisany certyfikat do interfejsu GUI programu Data Protection for VMware vSphere.

### Uzyskiwanie dostępu do magazynu kluczy:

Certyfikaty są przechowywane w magazynie kluczy Java. Zawartość magazynu kluczy jest chroniona za pomocą hasła. Aby manipulować certyfikatami w magazynie kluczy, należy uzyskać dostęp do magazynu kluczy.

### O tym zadaniu

Domyślny certyfikat samopodpisany i hasło magazynu kluczy są generowane automatycznie podczas instalacji, przez co użytkownik nie zna hasła początkowego.

Wykonaj poniższą procedurę, aby zastąpić oryginalny magazyn kluczy nowym magazynem kluczy i nowym certyfikatem samopodpisany. Nowy magazyn kluczy jest chroniony hasłem określonym przez użytkownika.

Jeśli już znasz hasło magazynu kluczy, pomiń tę procedurę.

### Procedura

1. Zatrzymaj usługę interfejsu GUI programu Data Protection for VMware vSphere.
2. Z poziomu wiersza komend przejdź do katalogu magazynu kluczy.
  - W systemie Linux: /opt/tivoli/tsm/tdpvmware/common/webserver/usr/servers/veProfile/resources/security/
  - W systemie Windows: C:\IBM\SpectrumProtect\webserver\usr\servers\veProfile\resources\security\
3. Utwórz kopię zapasową pliku kluczy (key.jks), zmieniając jego nazwę lub przenosząc go do innego miejsca.
4. Utwórz nowy magazyn kluczy i nowy certyfikat samopodpisany, wprowadzając następującą komendę:

```
keytool -genkeypair -alias vekey -dname
CN=nazwa_fqdn,OU=Tivoli Storage Manager for VMware,O=IBM -keyalg RSA
-sigalg SHA256withRSA -keysize 2048 -validity dni -keystore
key.jks -storepass hasło -keypass hasło
```

Gdzie:

**-dname CN=nazwa\_fqdn,OU=Tivoli Storage Manager for VMware,O=IBM**  
*nazwa\_fqdn* oznacza nazwę DNS lub pełną nazwę domeny komputera, na którym zainstalowano interfejs GUI programu Data Protection for VMware vSphere.

**-validity dni**  
Okres ważności certyfikatu.

### **-storepass *hasło***

Hasło magazynu kluczy. Należy zapamiętać to hasło w celu użycia w przyszłości.

### **-keypass *hasło***

Hasło klucza prywatnego dla certyfikatu. To hasło musi być zgodne z hasłem magazynu kluczy.

5. Zakoduj hasło magazynu kluczy za pomocą narzędzia **securityUtility**. Wprowadź poniższą komendę.

- W systemie Linux: `/opt/tivoli/tsm/tdpvmware/common/webserver/bin/securityUtility encode`
- W systemie Windows: `C:\IBM\SpectrumProtect\webserver\bin\securityUtility.bat encode`

Po wyświetleniu zachęty wprowadź hasło magazynu kluczy, a następnie zapisz uzyskane dane (na przykład skopiuj je do schowka).

6. Otwórz plik `bootstrap.properties` w edytorze i dla właściwości `veProfile.keystore.pswd` ustaw zakodowaną wartość uzyskaną w poprzednim kroku. Plik `bootstrap.properties` znajduje się w następującym miejscu:

- W systemie Linux: `/opt/tivoli/tsm/tdpvmware/common/webserver/usr/servers/veProfile/`
- W systemie Windows: `C:\IBM\SpectrumProtect\webserver\usr\servers\veProfile\`

7. Uruchom usługę interfejsu GUI programu Data Protection for VMware vSphere.

### **Odsyłacze pokrewne:**

“Uruchamianie usług dla produktu Data Protection for VMware i ich działanie” na stronie 87

### **Tworzenie żądania podpisania certyfikatu:**

Po uzyskaniu dostępu do magazynu kluczy należy utworzyć żądanie podpisania certyfikatu (CSR).

### **Procedura**

Aby utworzyć żądanie CSR, wykonaj następujące kroki:

1. Z poziomu wiersza komend przejdź do katalogu magazynu kluczy.
  - W systemie Linux: `/opt/tivoli/tsm/tdpvmware/common/webserver/usr/servers/veProfile/resources/security/`
  - W systemie Windows: `C:\IBM\SpectrumProtect\webserver\usr\servers\veProfile\resources\security\`
2. Utwórz nowy certyfikat, wprowadzając następującą komendę:  
`keytool -genkeypair -alias klucz -dname CN=nazwa_fqdn,OU=jednostka,O=organizacja -keyalg RSA -sigalg SHA256withRSA -keysize 2048 -validity dni -keystore key.jks -storepass hasło -keypass hasło`

Gdzie:

#### **-alias *klucz***

*klucz* jest unikalnym aliasem, który identyfikuje certyfikat w magazynie kluczy. Jego nazwa jest zmieniana po odebraniu podpisanego certyfikatu.

#### **-dname CN=*nazwa\_fqdn*,OU=*jednostka*,O=*organizacja***

*nazwa\_fqdn* oznacza nazwę DNS lub pełną nazwę domeny komputera, na którym zainstalowano interfejs GUI Data Protection for VMware vSphere.

*jednostka i organizacja to informacje o organizacji, które są wymagane przez strategię lub ośrodek certyfikacji.*

**-validity dni**

Okres ważności certyfikatu.

**-storepass hasło**

Hasło magazynu kluczy. Jeśli nie znasz lub nie pamiętasz hasła magazynu kluczy, patrz sekcja “Uzyskiwanie dostępu do magazynu kluczy” na stronie 65.

**-keypass hasło**

Hasło klucza prywatnego dla certyfikatu. To hasło musi być zgodne z hasłem magazynu kluczy.

3. Utwórz żądanie CSR, wprowadzając następującą komendę:

```
keytool -certreq -alias klucz -file certreq.pem -keystore key.jks
```

Gdzie:

**-alias *klucz***

Alias certyfikatu z poprzedniego kroku.

**-file *certreq.pem***

Plik do zapisania żądania podpisania certyfikatu.

**Wysyłanie żądania podpisania certyfikatu do ośrodka certyfikacji:**

Po utworzeniu żądania certyfikatu (*certreq.pem*) należy je wysłać do ośrodka certyfikacji w celu podpisania. Należy wykonać instrukcje uzyskane od ośrodka certyfikacji.

**Odbieranie podpisanego certyfikatu:**

Po uzyskaniu podpisanego certyfikatu od ośrodka certyfikacji (CA) należy umieścić ten certyfikat w magazynie kluczy.

**Procedura**

Aby odebrać podpisany certyfikat, wykonaj następujące kroki:

1. Z poziomu wiersza komend przejdź do katalogu magazynu kluczy.
  - W systemie Linux: */opt/tivoli/tsm/tdpvmware/common/webserver/usr/servers/veProfile/resources/security/*
  - W systemie Windows: *C:\IBM\SpectrumProtect\webserver\usr\servers\veProfile\resources\security\*
2. Skopiuj pliki odebrane od ośrodka CA do tego miejsca. Wśród tych plików znajduje się certyfikat główny ośrodka CA, certyfikaty pośrednie ośrodka CA (jeśli istnieją) i podpisany certyfikat dla interfejsu GUI programu Data Protection for VMware vSphere.
3. Zatrzymaj usługę interfejsu GUI programu Data Protection for VMware vSphere.
4. Utwórz kopię zapasową pliku kluczy (*key.jks*), kopiując go pod inną nazwą lub do innego miejsca.
5. Zimportuj certyfikaty pośrednie ośrodka CA (jeśli istnieją), używając poniższej komendy. Jeśli zostanie wyświetlona zachęta służąca do potwierdzenia zaufania certyfikatów, odpowiedz *yes* (tak). W razie potrzeby powtórz ten krok dla wielu certyfikatów pośrednich.

```
keytool -importcert -alias pośredni_ošrodka_CA -file intermediate.pem -keystore key.jks -storepass hasło
```

Gdzie:

**-alias** *pośredni\_ośrodka\_CA*

Unikalny alias, który identyfikuje certyfikat w magazynie kluczy. Każdy certyfikat pośredni musi mieć unikalny alias.

**-file** *intermediate.pem*

Plik certyfikatu pośredniego uzyskany z ośrodka CA.

**-storepass** *hasło*

Hasło magazynu kluczy.

6. Zainportuj certyfikat główny ośrodka CA, wprowadzając następującą komendę. Jeśli zostanie wyświetlona zachęta służąca do potwierdzenia zaufania certyfikatu, odpowiedz *yes* (tak).

```
keytool -importcert -alias certyfikat_główny_CA -file root.pem -keystore
key.jks -storepass hasło
```

Gdzie:

**-alias** *certyfikat\_główny\_CA*

Unikalny alias, który identyfikuje certyfikat w magazynie kluczy.

**-file** *root.pem*

Plik certyfikatu głównego uzyskany z ośrodka CA.

**-storepass** *hasło*

Hasło magazynu kluczy.

7. Zainportuj certyfikat podpisany, wprowadzając następującą komendę:

```
keytool -importcert -alias klucz -file signedcert.pem -keystore
key.jks -storepass hasło
```

Gdzie:

**-alias** *klucz*

Alias certyfikatu podpisanego. Alias musi być taki sam, jak alias użyty podczas generowania żądania podpisania certyfikatu (CSR).

**-file** *signedcert.pem*

Plik certyfikatu podpisanego odebrany z ośrodka CA.

**-storepass** *hasło*

Hasło magazynu kluczy.

8. Usuń istniejący certyfikat, który zawiera alias **vekey**:

```
keytool -delete -alias vekey -keystore key.jks -storepass hasło
```

Gdzie **-storepass** *hasło* oznacza hasło magazynu kluczy.

9. Zmień nazwę certyfikatu podpisanego na **vekey**:

```
keytool -changealias -alias klucz -destalias vekey -keystore
key.jks -storepass hasło
```

Gdzie:

**-alias** *klucz*

Alias certyfikatu podpisanego.

**-storepass** *hasło*

Hasło magazynu kluczy.

10. Uruchom usługę interfejsu GUI programu Data Protection for VMware vSphere.

**Odsyłacze pokrewne:**

“Uruchamianie usług dla produktu Data Protection for VMware i ich działanie” na stronie 87

---

## Wymagania dotyczące uprawnień użytkownika serwera VMware vCenter

Do uruchamiania operacji programu Data Protection for VMware wymagane są określone uprawnienia użytkownika serwera VMware vCenter.

### Uprawnienia serwera vCenter wymagane do ochrony centrów przetwarzania danych VMware przy użyciu widoku przeglądarki WWW dla interfejsu GUI Data Protection for VMware vSphere

ID użytkownika serwera vCenter, który loguje się do widoku przeglądarki dla interfejsu GUI Data Protection for VMware vSphere,

musi mieć uprawnienia środowiska VMware wystarczające do wyświetlania treści dla centrum przetwarzania danych, które jest zarządzane za pomocą interfejsu GUI.

Na przykład środowisko VMware vSphere zawiera pięć centrów przetwarzania danych. Użytkownik "jenn" ma wystarczające uprawnienia tylko dla dwóch z tych centrów przetwarzania danych. W związku z tym tylko te dwa centra przetwarzania danych, dla których istnieją wystarczające uprawnienia, są widoczne dla użytkownika "jenn" w widokach. Pozostałe trzy centra przetwarzania danych (dla których użytkownik "jenn" nie ma uprawnień) nie są widoczne dla tego użytkownika.

Serwer VMware vCenter definiuje zestaw uprawnień łącznie jako rolę. Rola jest stosowana do obiektu dla konkretnego użytkownika lub grupy w celu utworzenia uprawnienia. W kliencie WWW VMware vSphere należy utworzyć rolę z zestawem uprawnień. Aby utworzyć rolę serwera vCenter dla operacji tworzenia i odtwarzania kopii zapasowych, należy użyć funkcji **Add a Role** (Dodaj rolę) klienta VMware vSphere.

Aby propagować uprawnienia do wszystkich centrów przetwarzania danych na serwerze vCenter, należy określić serwer vCenter i zaznaczyć pole wyboru **propagate to children** (propaguj do elementów potomnych). W przeciwnym razie można ograniczyć te uprawnienia, jeśli ta rola zostanie przypisana tylko do wymaganych centrów przetwarzania danych z zaznaczonym polem wyboru **propagate to children** (propaguj do elementów potomnych). Wymuszenie dla interfejsu GUI przeglądarki odbywa się na poziomie centrum przetwarzania danych.

W poniższym przykładzie przedstawiono sposób kontroli dostępu do centrów przetwarzania danych dla dwóch grup użytkowników środowiska VMware. Najpierw należy utworzyć rolę zawierającą wszystkie uprawnienia zdefiniowane w nocie technicznej 7047438. Zbiór uprawnień w tym przykładzie jest identyfikowany za pomocą roli o nazwie "TDPVMwareManage". Grupa 1 wymaga dostępu do zarządzania maszynami wirtualnymi dla centrów przetwarzania danych Primary1\_DC i Primary2\_DC. Grupa 2 wymaga dostępu do zarządzania maszynami wirtualnymi dla centrów przetwarzania danych Secondary1\_DC i Secondary2\_DC.

Dla grupy 1 należy przypisać rolę "TDPVMwareManage" do centrów przetwarzania danych Primary1\_DC i Primary2\_DC. Dla grupy 2 należy przypisać rolę "TDPVMwareManage" do centrów przetwarzania danych Secondary1\_DC i Secondary2\_DC.

Użytkownicy w każdej grupie użytkowników środowiska VMware mogą używać interfejsu GUI programu Data Protection for VMware do zarządzania maszynami wirtualnymi tylko w odpowiadających im centrach przetwarzania danych.

**Wskazówka:** Podczas tworzenia roli należy rozważyć dodanie dodatkowych uprawnień do roli, która może być później potrzebna do wykonania innych czynności na obiektach.

## Uprawnienia serwera vCenter wymagane do użycia narzędzia przenoszenia danych

Narzędzie przenoszenia danych programu IBM Spectrum Protect, które jest zainstalowane na serwerze kopii zapasowych vStorage (węzeł narzędzia przenoszenia danych), wymaga opcji VMCUser i VMCPw. Opcja VMCUser określa ID użytkownika serwera vCenter lub ESX, który ma wykonywać operacje tworzenia i odtwarzania kopii zapasowych, a także odpytywania. Wymagane uprawnienia, które są przypisane do tego ID użytkownika (VMCUser), zapewniają, że klient może uruchamiać operacje na maszynie wirtualnej i w środowisku VMware. Ten ID użytkownika musi mieć uprawnienia środowiska VMware, które są opisane w powyższej nocie technicznej.

Aby utworzyć rolę serwera vCenter dla operacji tworzenia i odtwarzania kopii zapasowych, należy użyć funkcji **Add a Role** (Dodaj rolę) klienta VMware vSphere. Podczas dodawania uprawnień dla tego ID użytkownika (VMCUser) należy wybrać opcję **propagate to children** (propaguj do elementów potomnych). Ponadto należy rozważyć dodanie innych uprawnień do tej roli na potrzeby czynności innych niż tworzenie i odtwarzanie kopii zapasowych. Wymuszanie dla opcji VMCUser odbywa się na poziomie obiektu najwyższego poziomu.

## Uprawnienia serwera vCenter wymagane do ochrony centrów przetwarzania danych VMware przy użyciu widoku wtyczki klienta IBM Spectrum Protect vSphere dla interfejsu GUI Data Protection for VMware vSphere

Wtyczka klienta IBM Spectrum Protect vSphere wymaga użycia zestawu uprawnień oddzielnych w stosunku do uprawnień wymaganych do zalogowania się do interfejsu GUI.

Podczas instalowania następujące uprawnienia niestandardowe są tworzone dla wtyczki klienta IBM Spectrum Protect vSphere:

- **Centrum przetwarzania danych > IBM Data Protection**
- **Globalne > Skonfiguruj IBM Data Protection**

Uprawnienia niestandardowe, które są wymagane dla wtyczki klienta IBM Spectrum Protect vSphere, są rejestrowane jako oddzielne rozszerzenie. Kluczem rozszerzenia uprawnień jest `com.ibm.tsm.tdpvmware.IBMDataProtection.privileges`.

Te uprawnienia umożliwiają administratorowi VMware włączanie i wyłączanie dostępu do treści wtyczki klienta IBM Spectrum Protect vSphere. Tylko użytkownicy z tymi uprawnieniami niestandardowymi dla wymaganego obiektu środowiska VMware mogą uzyskać dostęp do treści wtyczki klienta IBM Spectrum Protect vSphere. Jeden komponent wtyczki klienta IBM Spectrum Protect vSphere jest zarejestrowany dla każdego serwera vCenter i jest współużytkowany przez wszystkie hosty interfejsu GUI skonfigurowane do obsługi serwera vCenter.

W kliencie WWW środowiska VMware vSphere należy utworzyć rolę dla użytkowników, którzy mogą wykonywać funkcje ochrony danych dla maszyn wirtualnych za pomocą komponentu wtyczki klienta IBM Spectrum Protect vSphere. Dla tej roli, oprócz uprawnień standardowej roli administratora maszyn wirtualnych wymaganej przez klienta WWW, należy określić uprawnienie **Centrum przetwarzania danych > IBM Data Protection**. Dla każdego centrum przetwarzania danych należy przypisać tę rolę każdemu użytkownikowi lub każdej grupie użytkowników, której chcesz nadać uprawnienie użytkownika służące do zarządzania maszynami wirtualnymi.

Dla użytkownika wymagane jest uprawnienie **Globalne > IBM Data Protection** na poziomie serwera vCenter. To uprawnienie umożliwia użytkownikowi zarządzanie połączeniem między



serwerem vCenter i serwerem WWW interfejsu GUI programu Data Protection for VMware vSphere, a także edytowanie i czyszczenie tego połączenia. To uprawnienie należy przypisać administratorom, którzy są zaznajomieni z interfejsem GUI programu Data Protection for VMware vSphere chroniącym ich odpowiedni serwer vCenter. Połączeniami komponentu wtyczka klienta IBM Spectrum Protect vSphere można zarządzać na stronie Połączenia rozszerzenia.

W poniższym przykładzie przedstawiono sposób kontroli dostępu do centrów przetwarzania danych dla dwóch grup użytkowników. Grupa 1 wymaga dostępu do zarządzania maszynami wirtualnymi dla centrów przetwarzania danych NewYork\_DC i Boston\_DC. Grupa 2 wymaga dostępu do zarządzania maszynami wirtualnymi dla centrów przetwarzania danych LosAngeles\_DC i SanFrancisco\_DC.

W kliencie środowiska VMware vSphere utwórz na przykład rolę "IBMDDataProtectManage", przypisz uprawnienia standardowej roli administratora maszyn wirtualnych, a także uprawnienie **Datacenter > IBM Data Protection**.

Dla grupy 1 należy przypisać rolę "IBMDDataProtectManage" do centrów przetwarzania danych NewYork\_DC i Boston\_DC. Dla grupy 2 należy przypisać rolę "IBMDDataProtectManage" do centrów przetwarzania danych LosAngeles\_DC i SanFrancisco\_DC.

Użytkownicy w każdej grupie mogą używać komponentu wtyczka klienta IBM Spectrum Protect vSphere w kliencie WWW środowiska vSphere do zarządzania maszynami wirtualnymi tylko w odpowiadających im centrach przetwarzania danych.

## Problemy związane z niewystarczającymi uprawnieniami

Jeśli użytkownik przeglądarki WWW nie ma wystarczających uprawnień do dowolnego centrum przetwarzania danych, dostęp do widoku jest blokowany. Wyświetlany jest natomiast komunikat o błędzie GVM2013E z informacją, że użytkownik nie jest upoważniony do dostępu do zarządzanych centrów przetwarzania danych ze względu na niewystarczające uprawnienia. Dostępne są też inne nowe komunikaty informujące użytkowników o problemach wynikających z niewystarczających uprawnień. Aby rozwiązać wszelkie problemy związane z uprawnieniami, należy skonfigurować rolę użytkownika zgodnie z opisem w poprzednich sekcjach. Rola użytkownika musi mieć wszystkie uprawnienia określone w tabeli wymaganych uprawnień dla ID użytkownika serwera vCenter i narzędzia przenoszenia danych, a uprawnienia te muszą być stosowane na poziomie centrum przetwarzania danych za pomocą pola wyboru **propagate to children** (propaguj do elementów potomnych).

Jeśli użytkownik komponentu wtyczka klienta IBM Spectrum Protect vSphere nie ma wystarczających uprawnień do centrum przetwarzania danych, funkcje ochrony danych dla tego centrum przetwarzania danych i jego zawartości są niedostępne w rozszerzeniu.

Jeśli ID użytkownika programu IBM Spectrum Protect (określony za pomocą opcji **VMCUser**) ma uprawnienia niewystarczające dla operacji tworzenia i odtwarzania kopii zapasowych, zostanie wyświetlony następujący komunikat:

ANS9365E Błąd interfejsu API VMware vStorage.  
"Odmówiono uprawnienia do wykonania tej operacji."

Jeśli ID użytkownika programu IBM Spectrum Protect ma uprawnienia niewystarczające do wyświetlenia maszyny, zostaną wyświetlone następujące komunikaty:

Uruchomiono komendę Backup VM. łączna liczba maszyn wirtualnych do przetworzenia: 1  
ANS4155E Nie można znaleźć maszyny wirtualnej 'tango' na serwerze VMware.  
ANS4148E Niepowodzenie tworzenia pełnej kopii zapasowej maszyny wirtualnej 'foxtrot'  
z kodem powrotu 4390

Dodatkowe informacje dotyczące wykorzystania uprawnień zawiera serwis WWW **vCenter Server privileges required for the Data Protection for VMware vSphere GUI and data mover**.

Aby za pomocą serwera VMware Virtual Center Server odtworzyć informacje zawarte w dzienniku dotyczące problemów z uprawnieniami, wykonaj następujące kroki:

1. W obszarze vCenter Server Settings (Ustawienia serwera vCenter) wybierz opcję **Logging Options** (Opcje rejestrowania) i dla parametru **vCenter Logging** (Rejestrowanie przez serwer vCenter) ustaw opcję **Trivia (Trivia)**.
2. Ponownie wygeneruj błąd dotyczący uprawnień.
3. Zresetuj parametr **vCenter Logging** (Rejestrowanie serwera vCenter) do jego poprzedniej wartości, aby zapobiec rejestrowaniu w dzienniku nadmiernej ilości informacji.
4. W oknie System Logs (Dzienniki systemowe) znajdź najnowszy dziennik serwera vCenter (vpxd-wxyz.log) i znajdź w nim łańcuch NoPermission. Na przykład:  
[2011-04-27 15:15:35.955 03756 verbose 'App'] [VpxVmomi] Invoke error:  
vim.VirtualMachine.createSnapshot session: 92324BE3-CD53-4B5A-B7F5-96C5FAB3F0EE  
Throw: vim.fault.NoPermission

Ten komunikat dziennika wskazuje, że ID użytkownika nie miał uprawnień wystarczających do utworzenia obrazu stanu (createSnapshot).

---

## Role użytkowników w interfejsie GUI Data Protection for VMware vSphere

Dostępność funkcji interfejsu GUI Data Protection for VMware vSphere jest oparta na poziomie uprawnień przypisanym do identyfikatora administratora programu IBM Spectrum Protect.

Identyfikator administratora musi być zgodny z nazwą węzła. We wcześniejszych wersjach produktu komenda **REGISTER NODE** automatycznie tworzyła identyfikator użytkownika administracyjnego, którego nazwa była zgodna z nazwą węzła. Od wersji 8.1 produktu IBM Spectrum Protect komenda serwera **REGISTER NODE** nie tworzy automatycznie identyfikatora użytkownika administracyjnego zgodnego z nazwą węzła.

Podczas rejestrowania nowego węzła administrator serwera IBM Spectrum Protect musi użyć parametru **userid** w komendzie serwera **REGISTER NODE**:

```
REGISTER NODE nazwa_węzła hasło userid=id_użytkownika
```

Nazwa węzła i identyfikator użytkownika administracyjnego muszą być takie same. Na przykład:

```
REGISTER NODE wez_a m0jeha$lo userid=wez_a
```

Domyślnie węzeł ten ma uprawnienie właściciela klienta.

Zadania, które można uruchomić za pomocą interfejsu GUI Data Protection for VMware vSphere, zależą od klasy uprawnienia przypisanej do identyfikatora administratora.

Gdy identyfikator administratora nie ma nieograniczonych uprawnień domeny strategii, nie można zarejestrować nowych węzłów ani ustawić relacji proxy w serwerze IBM Spectrum

Protect. W przypadku kontynuowania bez podawania identyfikatora administratora, zostanie utworzony skrypt makro, który należy uruchomić na serwerze IBM Spectrum Protect.

Żądanie podania identyfikatora administratora produktu IBM Spectrum Protect pojawia się podczas konfigurowania interfejsu GUI Data Protection for VMware vSphere. Ta tabela zawiera funkcje, których dostępność zależy od klasy uprawnień przypisanej do tego identyfikatora:

- Wartość Tak wskazuje na dostępność funkcji dla danej roli użytkownika.
- Wartość Nie wskazuje, że funkcja nie jest dostępna dla danej roli użytkownika.

Aby wyświetlić bieżącą rolę użytkownika serwera interfejsu GUI Data Protection for VMware vSphere, umieść kursor nad używanym identyfikatorem użytkownika na pasku nawigacyjnym.

*Tabela 11. Funkcje dostępne w zależności od uprawnień identyfikatora administratora produktu IBM Spectrum Protect*

|                                                                     | <b>Operator</b>                                                 | <b>Operator z raportowaniem</b>                                                                                                                 | <b>Administrator ograniczony</b>                                                                                                                                            | <b>Administrator</b>                                |
|---------------------------------------------------------------------|-----------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------|
| <b>Podsumowanie</b>                                                 | Uruchom teraz<br>tworzenie i<br>odtworzenie kopii<br>zapasowych | Operator plus<br>raportowanie                                                                                                                   | Operator plus<br>operacje<br>planowania i<br>raportowania dla<br>podanych domen<br>strategii                                                                                | Wszystkie role, w tym<br>konfiguracja<br>początkowa |
| <b>Klasa uprawnień administratora programu IBM Spectrum Protect</b> | Brak                                                            | Jedna z następujących klas uprawnień: <ul style="list-style-type: none"> <li>• Pamięć masowa</li> <li>• Operator</li> <li>• Analityk</li> </ul> | Strategia (ograniczona) lub jedna z następujących klas uprawnień: <ul style="list-style-type: none"> <li>• Pamięć masowa</li> <li>• Operator</li> <li>• Analityk</li> </ul> | Strategia (nieograniczona) lub system               |

#### Karta Kopia zapasowa

|                                                     |                  |                  |                               |     |
|-----------------------------------------------------|------------------|------------------|-------------------------------|-----|
| Zarządzaj kopiami zapasowymi tworzonymi natychmiast | Tak              | Tak              | Tak                           | Tak |
| Zarządzaj zaplanowanymi kopiami zapasowymi          | Nie <sup>1</sup> | Nie <sup>1</sup> | Tak, w ramach domen strategii | Tak |
| Wyświetl kopie zapasowe tworzone natychmiast        | Tak              | Tak              | Tak                           | Tak |
| Wyświetl zaplanowane kopie zapasowe                 | Nie              | Tak              | Tak                           | Tak |
| Usuń zaplanowane kopie zapasowe                     | Nie              | Nie              | Tak, w ramach domen strategii | Tak |

Tabela 11. Funkcje dostępne w zależności od uprawnień identyfikatora administratora produktu IBM Spectrum Protect (kontynuacja)

|                                                                                                                                   | Operator         | Operator z raportowaniem | Administrator ograniczony | Administrator |
|-----------------------------------------------------------------------------------------------------------------------------------|------------------|--------------------------|---------------------------|---------------|
| <b>Karta Odtwarzanie</b>                                                                                                          |                  |                          |                           |               |
| Uruchom zadanie odtwarzania                                                                                                       | Tak              | Tak                      | Tak                       | Tak           |
| <b>Karta Raporty</b>                                                                                                              |                  |                          |                           |               |
| Zdarzenia                                                                                                                         | Nie              | Tak                      | Tak                       | Tak           |
| Ostatnie zadania                                                                                                                  | Tak              | Tak                      | Tak                       | Tak           |
| Status kopii zapasowej                                                                                                            | Nie              | Tak                      | Tak                       | Tak           |
| Ochrona aplikacji                                                                                                                 | Nie              | Tak                      | Tak                       | Tak           |
| Zajętość centrum przetwarzania danych                                                                                             | Nie              | Tak                      | Tak                       | Tak           |
| <b>Karta Konfiguracja</b>                                                                                                         |                  |                          |                           |               |
| Rejestracja węzła<br>Status konfiguracji<br>-> ( <b>Uruchom kreatora konfiguracji</b> )                                           | Nie              | Nie                      | Nie <sup>2</sup>          | Tak           |
| Zmień informacje autoryzacyjne ID administratora IBM Spectrum Protect<br>Status konfiguracji<br>-> ( <b>Edytuj konfigurację</b> ) | Tak              | Tak                      | Tak                       | Tak           |
| Zmień hasło węzła VMCLI<br>Status konfiguracji<br>-> ( <b>Edytuj konfigurację</b> )                                               | Nie              | Nie                      | Tak                       | Tak           |
| Zmień domenę GUI<br>Status konfiguracji<br>-> ( <b>Edytuj konfigurację</b> )                                                      | Tak <sup>3</sup> | Tak <sup>3</sup>         | Tak <sup>3</sup>          | Tak           |
| Zmień węzły narzędzia przenoszenia danych<br>Status konfiguracji<br>-> ( <b>Edytuj konfigurację</b> )                             | Nie              | Nie                      | Nie <sup>2</sup>          | Tak           |

Tabela 11. Funkcje dostępne w zależności od uprawnień identyfikatora administratora produktu IBM Spectrum Protect (kontynuacja)

|                                                                                           | Operator | Operator z raportowaniem | Administrator ograniczony | Administrator |
|-------------------------------------------------------------------------------------------|----------|--------------------------|---------------------------|---------------|
| Zmień węzły proxy podłączania<br>Status konfiguracji<br>-> ( <b>Edytuj konfigurację</b> ) | Nie      | Nie                      | Nie <sup>2</sup>          | Tak           |

1. Nie można zarejestrować węzła, ponieważ wymagana jest nieograniczona strategia domeny.
2. Można dodawać i usuwać centra przetwarzania danych VMware i rejestrować węzły centrów przetwarzania danych.

Aby wyświetlić poziom uprawnień administratora programu IBM Spectrum Protect i odpowiadającej mu roli w interfejsie GUI Data Protection for VMware vSphere:

1. Przejdź do okna Konfiguracja.
2. Kliknij opcję **Edytuj konfigurację**.
3. Odpowiednie informacje są wyświetlane na stronie Informacje autoryzacyjne serwera Spectrum Protect.

**Ważne:**

- Jeśli poziom uprawnień administratora IBM Spectrum Protect ulegnie zmianie na serwerze IBM Spectrum Protect, należy zrestartować interfejs GUI Data Protection for VMware vSphere, aby odzwierciedlić te zmiany.
- Przy zmianie roli użytkownika, kliknij przycisk **OK**, aby zapisać zmiany przed przejściem do kolejnej strony Ustawień konfiguracyjnych lub przed próbą wprowadzenia innych zmian w konfiguracji. W przeciwnym razie zmiany w roli użytkownika nie odniosą skutku.

## Klucze rejestracji interfejsu GUI programu Data Protection for VMware

W zależności od opcji wybranych podczas instalacji można uzyskać dostęp do interfejsu GUI programu Data Protection for VMware za pomocą różnych metod. Klucze rejestracji są tworzone dla interfejsów GUI programu Data Protection for VMware.

Fraza “interfejs GUI programu Data Protection for VMware” dotyczy następujących interfejsów GUI:

- Interfejs GUI Data Protection for VMware vSphere, do którego dostęp jest realizowany za pomocą przeglądarki WWW
- Interfejs wtyczka klienta IBM Spectrum Protect vSphere w interfejsie GUI vSphere Web Client

Kluczem rejestracji wtyczki klienta IBM Spectrum Protect vSphere jest `com.ibm.tsm.tdpvmware.IBMDDataProtection`. Ten klucz jest rejestrowany po zaznaczeniu pola wyboru **Zarejestruj rozszerzenie vSphere Web Client** podczas instalacji. Pojedyncza instancja wtyczki klienta IBM Spectrum Protect vSphere jest rejestrowana na jednym serwerze vCenter.

Klucz rejestracji nie jest tworzony dla interfejsu GUI Data Protection for VMware vSphere, który jest dostępny za pomocą przeglądarki WWW.

Aby wyświetlić klucze rejestracji, zaloguj się do przeglądarki VMware Managed Object Browser (MOB). Po zalogowaniu się do przeglądarki MOB wybierz opcje

**Content**→**Extension Manager** (Treść → Menedżer rozszerzeń), aby wyświetlić klucze rejestracji.

---

## Konfigurowanie interfejsu GUI programu agent odtwarzania

W tej sekcji znajdują się instrukcje dotyczące sposobu konfigurowania interfejsu GUI programu agent odtwarzania dla operacji podłączania, odtwarzania plików i natychmiastowego odtwarzania.

### Zanim rozpocznieś

Podane czynności konfiguracyjne należy wykonać przed próbą wykonania operacji w interfejsie GUI programu agent odtwarzania.

**Ważne:** Informacje o tym, w jaki sposób można wykonywać czynności za pomocą interfejsu GUI agenta odtwarzania, są dostępne w pomocy elektronicznej instalowanej razem z interfejsem GUI. Kliknięcie opcji **Pomoc** w dowolnym oknie interfejsu GUI powoduje otwarcie pomocy elektronicznej zapewniającej asystę do wykonywanych czynności.

### Procedura

1. Zaloguj się do systemu, w którym mają być odtworzone pliki. W systemie musi być zainstalowany program agent odtwarzania.
2. Kliknij opcję **Wybierz serwer TSM** w interfejsie GUI agenta odtwarzania, aby nawiązać połączenie z serwerem IBM Spectrum Protect. Jeśli agent odtwarzania został zainstalowany w tym samym systemie co interfejs GUI Data Protection for VMware vSphere i aplikacje zostały pomyślnie skonfigurowane za pomocą kreatora konfiguracji interfejsu GUI Data Protection for VMware vSphere, obowiązują następujące warunki:
  - Węzeł narzędzia przenoszenia danych i serwer IBM Spectrum Protect są zapełniane w polu Serwer TSM agenta odtwarzania.
  - W panelu Informacje o serwerze TSM znajdują się następujące pola:
    - **Węzeł uwierzytelniania** zawiera listę dostępnych węzłów narzędzia przenoszenia danych.
    - **Węzeł docelowy** zawiera listę węzłów centrum przetwarzania danych dostępnych dla wybranego węzła narzędzia przenoszenia danych.

Jeśli za pomocą kreatora konfiguracji lokalnie został zdefiniowany tylko jeden węzeł narzędzia przenoszenia danych, program agent odtwarzania używa tego węzła do uwierzytelniania przy uruchamianiu. Program agent odtwarzania pamięta nazwę ostatniego węzła połączonego z serwerem IBM Spectrum Protect. Jeśli dla tego węzła (ostatni węzeł połączony z serwerem) jest wybrana opcja **Użyj dostępu po podaniu hasła**, do połączenia z serwerem IBM Spectrum Protect program agent odtwarzania użyje tych informacji autoryzacyjnych. Jeśli wcześniej nie nawiązano żadnego połączenia z serwerem IBM Spectrum Protect i w kreatorze skonfigurowano tylko jeden węzeł narzędzia przenoszenia danych i jeden węzeł centrum przetwarzania danych, program agent odtwarzania użyje tych informacji autoryzacyjnych do połączenia się z serwerem IBM Spectrum Protect.

Podaj następujące opcje:

#### Adres serwera

Podaj adres IP lub nazwę hosta IBM Spectrum Protect.

#### Port serwera

Wprowadź numer portu używany do komunikacji TCP/IP z serwerem.  
Domyślny numer portu: 1500.

Metoda dostępu do węzła:

### Asnodename

Wybierz tę opcję, aby używać węzła proxy w celu uzyskania dostępu do kopii zapasowych maszyn wirtualnych dostępnych w węźle docelowym. Węzeł proxy jest to węzeł, który ma uprawnienia do wykonywania operacji w imieniu węzła docelowego.

Zwykle administrator programu IBM Spectrum Protect używa komendy **grant proxynode** do utworzenia relacji między istniejącymi węzłami.

Po zaznaczeniu tej opcji należy wykonać następujące czynności:

- W polu **Węzeł docelowy** podaj nazwę węzła docelowego (węzła, w którym znajdują się kopie zapasowe maszyn wirtualnych).
- W polu **Węzeł uwierzytelniania** podaj nazwę węzła proxy.
- W polu **Hasło** podaj hasło węzła proxy.
- Kliknij przycisk **OK**, aby zapisać ustawienia i zamknąć okno dialogowe programu IBM Spectrum Protect.

Gdy używana jest ta metoda, użytkownik programu agent odtwarzania zna tylko hasło węzła proxy, a hasło węzła docelowego jest chronione.

### Fromnode

Wybierz tę opcję, aby użyć węzła z dostępem ograniczonym tylko do danych obrazu stanu określonych maszyn wirtualnych dostępnych w węźle docelowym.

Zwykle ten węzeł ma uprawnienia nadawane przez węzeł docelowy, który jest właścicielem kopii zapasowych maszyn wirtualnych (patrz komenda **set access**):

```
set access backup -TYPE=VM nazwa_wyświetlana_maszyny_wirtualnej
nazwa_węzła_podłączenia
```

Na przykład, następująca komenda nadaje węzłowi o nazwie **myMountNode** uprawnienia do odtwarzania plików z maszyny wirtualnej o nazwie **myTestVM**:

```
set access backup -TYPE=VM myTestVM myMountNode
```

Po zaznaczeniu tej opcji należy wykonać następujące czynności:

- W polu **Węzeł docelowy** podaj nazwę węzła docelowego (węzła, w którym znajdują się kopie zapasowe maszyn wirtualnych).
- W polu **Węzeł uwierzytelniania** podaj nazwę węzła z ograniczonym dostępem.
- W polu **Hasło** podaj hasło węzła z ograniczonym dostępem.
- Kliknij przycisk **OK**, aby zapisać ustawienia i zamknąć okno dialogowe programu IBM Spectrum Protect.

Gdy używana jest ta metoda, użytkownikowi wyświetlana jest pełna lista maszyn wirtualnych z kopiami zapasowymi. Odtworzyć można jednak tylko te maszyny wirtualne, do których węzeł ma nadane uprawnienia. Dodatkowo dane obrazu stanu nie są zabezpieczone przed utratą ważności na serwerze. Z tego względu natychmiastowe odtwarzanie nie jest obsługiwane w tej metodzie.

### Bezpośrednio

Wybierz tę opcję, aby wykonać uwierzytelnianie bezpośrednio w węźle docelowym (węźle, w którym znajdują się kopie zapasowe maszyn wirtualnych).

Po zaznaczeniu tej opcji należy wykonać następujące czynności:

- W polu **Węzeł uwierzytelniania** podaj nazwę węzła docelowego (węzła, w którym znajdują się kopie zapasowe maszyn wirtualnych).
- W polu **Hasło** podaj hasło węzła docelowego.

- c. Kliknij przycisk **OK**, aby zapisać ustawienia i zamknąć okno dialogowe programu IBM Spectrum Protect.

#### **Użyj dostępu po podaniu hasła**

Jeśli ta opcja jest wybrana i pole hasła jest puste, agent odtwarzania wykonuje uwierzytelnianie za pomocą istniejącego hasła przechowywanego w rejestrze. Jeśli ta opcja nie jest wybrana, hasło należy podać samodzielnie.

Aby użyć tej opcji, należy najpierw ustawić samodzielnie hasło początkowe dla węzła, którego dotyczy ta opcja. Podczas pierwszego nawiązywania połączenia z węzłem IBM Spectrum Protect należy podać hasło początkowe, wprowadzając je w polu **Hasło** i zaznaczając pole wyboru **Użyj dostępu po podaniu hasła**.

Jeśli jednak węzeł narzędzia przenoszenia danych jest używany jako **węzeł uwierzytelniania**, hasło może już być zapisane w rejestrze. W takiej sytuacji należy zaznaczyć pole wyboru **Użyj dostępu po podaniu hasła** i nie wprowadzać hasła.

agent odtwarzania wysłał do podanego serwera zapytanie o listę zabezpieczonych maszyn wirtualnych i wyświetla ją.

3. Ustaw poniższe opcje podłączania, tworzenia kopii zapasowej i odtwarzania, klikając opcję **Ustawienia**:

#### **Pamięć podręczna zapisu woluminu wirtualnego**

Agent odtwarzania, który jest uruchomiony na hoście proxy kopii zapasowej w systemie Windows, zapisuje zmiany danych powstałe podczas operacji natychmiastowego odtwarzania i podłączania. Zmiany te są zapisywane w woluminie wirtualnym w pamięci podręcznej zapisu. Domyślnie pamięć podręczna zapisu jest włączona i wskazuje ścieżkę `C:\ProgramData\Tivoli\TSM\TDPVMware\mount\`, a maksymalna wielkość pamięci podręcznej wynosi 90% dostępnego miejsca w wybranym folderze. Aby zapobiec zapełnieniu woluminu systemowego, zmień pamięć podręczną zapisu na ścieżkę w woluminie innym niż systemowy.

#### **Folder dla plików tymczasowych**

Podaj ścieżkę, w której będą zapisywane zmiany danych. Pamięć podręczna zapisu musi znajdować się na dysku lokalnym i nie można jej ustawić na ścieżkę folderu współużytkowanego. Jeśli pamięć podręczna zapisu jest wyłączona albo zapełniona, próba uruchomienia sesji natychmiastowego odtwarzania lub podłączania się nie powiedzie.

#### **Wielkość pamięci podręcznej**

Podaj wielkość pamięci podręcznej zapisu. Maksymalna dozwolona wielkość pamięci podręcznej wynosi 90% dostępnego miejsca w wybranym folderze.

**Ograniczenie:** Aby zapobiec przerwom podczas przetwarzania związanego z odtwarzaniem, należy wykluczyć ścieżkę pamięci podręcznej zapisu z wszystkich ustawień zabezpieczeń programu antywirusowego.

#### **Dostęp do danych**

Podaj typ danych, do których uzyskiwany jest dostęp. W przypadku używania urządzeń odłączonych (takich jak napędy taśm lub wirtualne biblioteki taśm), należy podać odpowiedni typ danych.

#### **Typ pamięci masowej**

Podaj jedno z następujących urządzeń pamięci masowej, z których ma być podłączony obraz stanu:



**Dysk/plik**

Obraz stanu jest podłączany z dysku lub z pliku. Jest to urządzenie domyślne.

**Taśma** Obraz stanu jest podłączany z puli pamięci masowej taśm. Gdy opcja ta jest wybrana, nie jest możliwe podłączanie wielu obrazów stanu ani uruchamianie operacji natychmiastowego odtwarzania.

**VTL** Obraz stanu jest podłączany z odłączonej wirtualnej biblioteki taśm. Uruchamianie współbieżnych sesji podłączania na tej samej wirtualnej bibliotece taśm jest obsługiwane.

**Uwaga:** Po zmianie typu pamięci masowej należy zrestartować usługę, aby zmiany odniosły skutek.

**Zablokuj ochronę przed utratą ważności**

W operacji podłączania obrazu stanu na serwerze IBM Spectrum Protect jest blokowany, aby zapobiec utracie jego ważności przez czas trwania operacji. Utrata ważności może wystąpić, ponieważ inny obraz stanu jest dodawany do sekwencji podłączonego obrazu stanu. Wartość ta określa, czy wyłączyć tę ochronę w operacji podłączania.

- Aby obraz stanu był chroniony przed utratą ważności, nie zaznaczaj tej opcji. Obraz stanu na serwerze IBM Spectrum Protect będzie blokowany przed utratą ważności podczas trwania podłączenia.
- Aby wyłączyć ochronę przed utratą ważności, zaznacz tę opcję. Ta opcja jest domyślnie zaznaczona. Obraz stanu na serwerze IBM Spectrum Protect nie będzie blokowany przed utratą ważności podczas trwania podłączenia. W wyniku obraz stanu może utracić ważność podczas trwania operacji podłączenia. Utrata ważności może prowadzić do nieoczekiwanych wyników i mieć ujemny wpływ na punkt podłączenia. Na przykład punkt podłączenia może stać się nieużyteczny albo generować błędy. Utrata ważności nie ma jednak wpływu na bieżącą aktywną kopię. Aktywna kopia nie może utracić ważności podczas trwania operacji.

Gdy obraz stanu jest na docelowym serwerze replikacji, nie może być zablokowany, ponieważ jest w trybie tylko do odczytu. Próba zablokowania przez serwer spowoduje, że operacja podłączenia się nie powiedzie. Aby tego uniknąć, wyłącz ochronę, zaznaczając tę opcję.

**Wielkość odczytu z wyprzedzeniem (w blokach 16 kB)**

Podaj liczbę dodatkowych bloków danych pobieranych z urządzenia pamięci masowej po wysłaniu żądania odczytu do pojedynczego bloku. Wartości domyślne są następujące:

- Dysk lub plik: 64
- Taśma: 1024
- Wirtualna biblioteka taśm: 64

Wartość maksymalna dla dowolnego urządzenia: 1024.

**Wielkość pamięci podręcznej odczytu z wyprzedzeniem (w blokach)**

Podaj wielkość pamięci podręcznej, w której są zapisywane odczytane dane dodatkowe. Wartości domyślne są następujące:

- Dysk lub plik: 10000
- Taśma: 75000
- Wirtualna biblioteka taśm: 10000

Ponieważ każdy obraz stanu ma własną pamięć podręczną, zaplanuj liczbę obrazów stanu, które są równocześnie podłączane lub odtwarzane. Łączna wielkość pamięci podręcznej nie może przekroczyć 75000 bloków.

#### **Limit czasu sterownika (sekundy)**

Ta wartość określa czas na przetwarzanie żądań danych sterownika systemu plików. Jeśli przetwarzanie nie zakończy się w tym czasie, żądanie jest anulowane i do sterownika systemu plików zwracany jest błąd. Zwiększenie tej wartości należy rozważyć w przypadku występowania błędów przekroczenia limitu czasu. Na przykład przekroczenia limitu czasu mogą występować, gdy sieć działa wolno, gdy urządzenie pamięci masowej jest bardzo obciążone lub gdy jednocześnie jest przetwarzanych wiele sesji podłączania lub natychmiastowego odtwarzania. Wartości domyślne są następujące:

- Dysk lub plik: 60
- Taśma: 180
- Wirtualna biblioteka taśm: 60

Kliknij przycisk **OK**, aby zapisać zmiany i wyjść z obszaru **Ustawienia**.

4. Upewnij się, że każdy węzeł serwera IBM Spectrum Protect (podany w opcji **Asnodename** i **Fromnode**) pozwala na usuwanie kopii zapasowych. Program agent odtwarzania tworzy podczas działania nieużywane obiekty tymczasowe. Opcja serwera **BACKDElete=Yes** umożliwia usuwanie takich obiektów, aby nie były one gromadzone w węźle.
  - a. Zaloguj się do serwera IBM Spectrum Protect i uruchom w wierszu komend sesję klienta administracyjnego:  
`dsmadm -id=admin -password=admin -dataonly=yes`
  - b. Wpisz następującą komendę:  
`Query Node <nazwa-węzła> Format=Detailed`

Upewnij się, że dla każdego węzła komenda wyświetla:

Backup Delete Allowed?: Yes  
(Usuwanie kopii zapasowej dozwolone?: Tak)

Jeśli tekst ten nie jest wyświetlany, zaktualizuj każdy węzeł, używając następującej komendy:

`UPDate Node <nazwa-węzła> BACKDElete=Yes`

Uruchom ponownie komendę **Query Node** dla każdego węzła, aby upewnić się, że usuwanie kopii zapasowych jest dozwolone.

5. Jeśli agent odtwarzania jest używany w sieci iSCSI i jeśli ten agent odtwarzania nie używa narzędzia przenoszenia danych, otwórz plik `C:\ProgramData\Tivoli\TSM\RecoveryAgent\mount\RecoveryAgent.conf` i podaj znacznik **[IMOUNT]** z parametrem **Target IP** (adres docelowy):  
[IMOUNT config]  
Target IP=<adres IP karty sieciowej systemu,  
który udostępnia cele iSCSI.>

Na przykład:

```
[General config]
param1
param2
...
[IMount config]
Target IP=9.11.153.39
```

Po dodaniu lub zmianie parametru Target IP zrestartuj interfejs GUI agenta odtwarzania lub jego interfejs wiersza komend.

## Włączanie bezpiecznej komunikacji od komponentu agent odtwarzania do serwera IBM Spectrum Protect

Jeśli serwer IBM Spectrum Protect jest skonfigurowany do używania protokołu SSL (Secure Sockets Layer) lub TLS (Transport Layer Security), można aktywować program agent odtwarzania do komunikacji z serwerem za pomocą tego protokołu.

### Zanim rozpocznieś

Przed rozpoczęciem konfigurowania bezpiecznej komunikacji z serwerem należy wziąć pod uwagę następujące kwestie:

- Każdy serwer z włączoną obsługą protokołu SSL musi mieć unikalny certyfikat. Certyfikat może mieć jeden z następujących typów:
  - Certyfikat, który został samopodpisany przez serwer.
  - Certyfikat, który został wystawiony przez ośrodek certyfikacji (CA). Certyfikat od ośrodka CA może pochodzić z firmy, takiej jak Symantec lub Thawte, ale może też być wewnętrznym certyfikatem przechowywanym w firmie.
- Ze względu na wydajność, protokołów SSL lub TLS należy używać tylko w tych sesjach, w których wymagane jest stosowanie zabezpieczeń. Należy rozważyć dodanie kolejnych procesorów w systemie serwera do obsługi zwiększonych wymagań.
- Aby klient mógł łączyć się z serwerem za pomocą protokołu TLS w wersji 1.2, algorytmem podpisu certyfikatu musi być algorytm Secure Hash Algorithm 1 (SHA-1) lub nowszy. W przypadku używania samopodpisanego certyfikatu dla serwera, który używa protokołu TLS w wersji 1.2, należy użyć certyfikatu **cert256.arm**. Może być konieczna zmiana domyślnego certyfikatu na serwerze przez administratora produktu IBM Spectrum Protect.
- Aby wyłączyć protokoły zabezpieczeń, które są mniej bezpieczne niż protokół TLS 1.2, należy dodać opcję **SSLDISABLELEGACYtls yes** do pliku **C:\windows\system32\fb.opt** lub **C:\Windows\SysWOW64\fb.opt**. Protokół TLS w wersji 1.2 lub nowszej chroni przed atakami przez szkodliwe programy.

### Włączanie bezpiecznej komunikacji przy użyciu certyfikatu samopodpisanego serwera IBM Spectrum Protect

Jeśli serwer IBM Spectrum Protect używa certyfikatu samopodpisanego, należy uzyskać kopię tego certyfikatu od administratora serwera i skonfigurować komponent agent odtwarzania do komunikacji z serwerem za pomocą protokołu SSL lub TLS.

### O tym zadaniu

Każdy serwer generuje własny certyfikat. Serwery w wersji 6.3 lub nowszej generują pliki o nazwie **cert256.arm**, jeśli serwer używa protokołu TLS w wersji 1.2 lub nowszej, lub **cert.arm**, jeśli serwer używa wcześniejszej wersji protokołu SSL lub TLS. W wersjach serwera wcześniejszych niż 6.3 generowane są pliki o nazwie **cert.arm** niezależnie od protokołu. Należy wybrać certyfikat, który jest ustawiony jako domyślny na serwerze.

Plik certyfikatu jest przechowywany na stacji roboczej serwera w katalogu instancji serwera. Na przykład: C:\IBM\tivoli\tsm\server\bin\cert256.arm. Jeśli plik certyfikatu nie istnieje, jest on tworzony podczas restartowania serwera z ustawionymi tymi opcjami.

## Procedura

Aby włączyć komunikację SSL lub TLS z agenta odtwarzania do serwera za pomocą certyfikatu samopodpisanego:

1. Dodaj ścieżkę do zasobów binarnych i bibliotek pakietu GSKit do zmiennej środowiskowej PATH na kliencie. Na przykład:  

```
set PATH=C:\Program Files\Common Files\Tivoli\TSM\api64\gsk8\bin\;
C:\Program Files\Common Files\Tivoli\TSM\api64\gsk8\lib64;%PATH%
```
2. Jeśli po raz pierwszy konfigurujesz protokół SSL lub TLS na kliencie, musisz utworzyć lokalną bazę danych kluczy klienta dsmcert.kdb. Z poziomu katalogu C:\Windows\SysWOW64 należy uruchomić komendę **gsk8capicmd\_64**, jak to pokazano w poniższym przykładzie:  

```
gsk8capicmd_64 -keydb -create -populate -db dsmcert.kdb -pw hasło -stash
```

Podane hasło jest używane do szyfrowania bazy danych kluczy. Hasło to jest automatycznie zapisywane jako zaszyfrowane w pliku ukrytym (dsmcert.sth). Plik ukryty jest używany przez klienta do pobierania hasła do bazy danych kluczy.

3. Uzyskaj certyfikat samopodpisany.
4. Zaimportuj certyfikat do bazy danych dsmcert.kdb. Do bazy danych dsmcert.kdb musisz zaimportować certyfikat dla każdego klienta. Z poziomu katalogu C:\Windows\SysWOW64 należy uruchomić komendę **gsk8capicmd\_64**, jak to pokazano w poniższym przykładzie:  

```
gsk8capicmd_64 -cert -add -db dsmcert.kdb -stashed
-label "Klucz samopodpisany serwera nazwa_serwera"
-file ścieżka_do_certyfikatu -format ascii -trust enable
```

Do bazy danych dsmcert.kdb można dodać wiele certyfikatów serwerów, aby klient mógł łączyć się z wieloma serwerami. Różne certyfikaty muszą mieć różne etykiety. Etykietom należy nadać użyteczne nazwy.

**Ważne:** W ramach odtwarzania serwera po awarii, jeśli certyfikat został utracony, serwer automatycznie generuje nowy certyfikat. Następnie każdy klient musi zaimportować ten nowy certyfikat.

5. Po dodaniu certyfikatu serwera do bazy danych dsmcert.kdb dodaj opcję **ssl yes** do pliku C:\Windows\SysWOW64\fb.opt i zaktualizuj wartość opcji **tcpport**.

### Ważne:

Serwer jest zwykle skonfigurowany do połączeń za pomocą protokołów SSL i TLS przy użyciu portu innego niż w przypadku połączeń innych niż połączenia za pomocą protokołów SSL i TLS. Jako wartości opcji **tcpport** nie należy podawać numeru portu innego niż numer portu dla protokołu SSL lub TLS. Jeśli wartość opcji **tcpport** będzie niepoprawna, agent odtwarzania nie będzie mógł połączyć się z serwerem.

Przy użyciu portu innego niż port dla protokołu SSL lub TLS nie można połączyć się z agentem odtwarzania, dla którego włączono obsługę protokołu SSL lub TLS. Nie można też użyć portu dla protokołu SSL lub TLS na potrzeby połączenia z agentem odtwarzania, dla którego nie włączono obsługi protokołu SSL lub TLS.

6. Ustaw poprawne porty SSL lub TLS w następujących plikach konfiguracyjnych agenta odtwarzania:
  - C:\ProgramData\Tivoli\TSM\RecoveryAgent\mount\RecoveryAgent.conf

- C:\ProgramData\Tivoli\TSM\RecoveryAgent\mount\RecoveryAgentDMNodes.conf

## Włączanie bezpiecznej komunikacji przy użyciu certyfikatu innej firmy

Jeśli serwer IBM Spectrum Protect korzysta z ośrodka certyfikacji (CA) innej firmy, należy uzyskać certyfikat główny ośrodka CA.

### O tym zadaniu

Jeśli certyfikat został wystawiony przez ośrodek CA, taki jak Symantec lub Thawte, klient jest gotowy do obsługi protokołu SSL lub TLS i można pominąć poniższe kroki konfiguracji. Aby znaleźć listę wstępnie zainstalowanych certyfikatów głównych ośrodka CA, należy wyszukać temat **Certyfikaty główne ośrodków certyfikacji** w Centrum Wiedzy IBM.

Jeśli certyfikat nie został wystawiony przez wstępnie zainstalowany certyfikat główny lub jest to wewnętrzny certyfikat ośrodka CA, który jest przechowywany w przedsiębiorstwie, należy skonfigurować agenta odtwarzania do komunikowania się z serwerem za pomocą protokołu SSL lub TLS.

### Procedura

Aby włączyć komunikację SSL lub TLS z agenta odtwarzania do serwera za pomocą certyfikatu ośrodka CA:

1. Dodaj ścieżkę do zasobów binarnych i bibliotek pakietu GSKit do zmiennej środowiskowej PATH. Na przykład:  

```
set PATH=C:\Program Files\Common Files\Tivoli\TSM\api64\gsk8\bin\;
C:\Program Files\Common Files\Tivoli\TSM\api64\gsk8\lib64;%PATH%
```
2. Jeśli po raz pierwszy konfigurujesz protokół SSL lub TLS na kliencie, musisz utworzyć lokalną bazę danych kluczy klienta dsmcert.kdb. Dla klientów, z poziomu katalogu C:\Windows\SysWOW64, należy uruchomić komendę **gsk8capicmd\_64**, jak to pokazano w poniższym przykładzie:  

```
gsk8capicmd_64 -keydb -create -populate -db dsmcert.kdb -pw hasło -stash
```

Podane hasło jest używane do szyfrowania bazy danych kluczy. Hasło to jest automatycznie zapisywane jako zaszyfrowane w pliku ukrytym (dsmcert.sth). Plik ukryty jest używany przez klienta do pobierania hasła do bazy danych kluczy.

3. Uzyskaj certyfikat ośrodka CA.
4. Zaimportuj certyfikat do bazy danych dsmcert.kdb. Do bazy danych dsmcert.kdb musisz zaimportować certyfikat dla każdego klienta. Dla klientów, z poziomu katalogu C:\Windows\SysWOW64, należy uruchomić komendę **gsk8capicmd\_64**, jak to pokazano w poniższym przykładzie:  

```
gsk8capicmd_64 -cert -add -db dsmcert.kdb -stashed -label "ośrodek certyfikacji XYZ"
-file ścieżka_do_certyfikatu_głównego_CA -format ascii -trust enable
```

Do bazy danych dsmcert.kdb można dodać wiele certyfikatów serwerów, aby klient mógł łączyć się z wieloma serwerami. Różne certyfikaty muszą mieć różne etykiety. Etykietom należy nadać użyteczne nazwy.

**Ważne:** W ramach odtwarzania serwera po awarii, jeśli certyfikat został utracony, serwer automatycznie generuje nowy certyfikat. Każdy klient musi zaimportować ten nowy certyfikat.

5. Po dodaniu certyfikatu serwera do bazy danych dsmcert.kdb dodaj opcję **ssl yes** do pliku C:\Windows\SysWOW64\fb.opt i zaktualizuj wartość opcji **tcpport**.

**Ważne:**

Serwer jest zwykle skonfigurowany do połączeń za pomocą protokołów SSL i TLS przy użyciu portu innego niż w przypadku połączeń innych niż połączenia za pomocą protokołów SSL i TLS. Jako wartości opcji `tcpport` nie należy podawać numeru portu innego niż numer portu dla protokołu SSL lub TLS. Jeśli wartość opcji `tcpport` będzie niepoprawna, agent odtwarzania nie będzie mógł połączyć się z serwerem.

Przy użyciu portu innego niż port dla protokołu SSL lub TLS nie można połączyć się z agentem odtwarzania, dla którego włączono obsługę protokołu SSL lub TLS. Nie można też użyć portu dla protokołu SSL lub TLS na potrzeby połączenia z agentem odtwarzania, dla którego nie włączono obsługi protokołu SSL lub TLS.

6. Ustaw poprawne porty SSL lub TLS w następujących plikach konfiguracyjnych agenta odtwarzania:
  - `C:\ProgramData\Tivoli\TSM\RecoveryAgent\mount\RecoveryAgent.conf`
  - `C:\ProgramData\Tivoli\TSM\RecoveryAgent\mount\RecoveryAgentDMNodes.conf`

---

## Ustawienia narodowe

Ustawienia narodowe określają język, który jest używany w interfejsach, komunikatach i pomocy elektronicznej.

### Interfejsy GUI programu Data Protection for VMware

Fraza "interfejs GUI programu Data Protection for VMware" dotyczy następujących interfejsów GUI:

- Interfejs GUI Data Protection for VMware vSphere, do którego dostęp jest realizowany za pomocą przeglądarki WWW
- Interfejs wtyczka klienta IBM Spectrum Protect vSphere w interfejsie GUI vSphere Web Client

Interfejsy GUI programu Data Protection for VMware nie obsługują działań w środowisku, które zawiera niespójne ustawienia narodowe między procesorami, na których działa interfejs GUI programu Data Protection for VMware, VMware vSphere Client i serwer IBM Spectrum Protect.

Należy podać takie same ustawienia narodowe dla systemów, w których działa interfejs GUI programu Data Protection for VMware, VMware vSphere Client i serwer IBM Spectrum Protect.

Jeśli dostęp do strony pomocy interfejsu GUI programu Data Protection for VMware jest realizowany za pomocą odsyłacza "Dowiedz się więcej" po raz pierwszy, pomoc zostanie wyświetlona w języku określonym w ustawieniach narodowych systemu, w którym działa ten interfejs GUI programu Data Protection for VMware. Pomoc nie jest wyświetlana w języku określonym za pomocą ustawień narodowych programu VMware vSphere Client przy pierwszym dostępie do tej pomocy. W tej sytuacji po wyświetleniu strony pomocy interfejsu GUI produktu Data Protection for VMware kliknij co najmniej dwa odsyłacze, a następnie zamknij okno pomocy. Przy następnym otwarciu pomocy za pomocą odsyłacza "Dowiedz się więcej" jest ona wyświetlana w języku określonym za pomocą ustawień narodowych programu VMware vSphere Client.

## Interfejs odtwarzania plików programu IBM Spectrum Protect

Język, w którym jest wyświetlana treść interfejsu i komunikatów, jest określany na podstawie ustawienia języka w przeglądarce WWW, która uzyskuje dostęp do interfejsu odtwarzania plików programu IBM Spectrum Protect.

Na potrzeby komunikatów o błędach rejestrowanych w pliku `fr_api.log` interfejs odtwarzania plików programu IBM Spectrum Protect używa języka określonego za pomocą ustawień narodowych systemu, w którym działa interfejs GUI Data Protection for VMware vSphere.

---

## Działanie plików dzienników

Podczas operacji instalowania, tworzenia kopii zapasowych, podłączania i odtwarzania program Data Protection for VMware tworzy i modyfikuje szereg plików dzienników.

Pliki dzienników programu Data Protection for VMware to pliki w formacie zwykłego tekstu o rozszerzeniu nazwy pliku `.sf`.

**Windows** Dzienniki są umieszczone w następującym katalogu:  
`%ALLUSERSPROFILE%\Tivoli\TSM\TDPVMware`  
Katalogi zawierają podkatalogi dla poszczególnych komponentów programu Data Protection for VMware. Na przykład podkatalogiem agenta odtwarzania jest `\mount`, a podkatalogiem interfejsu wiersza komend agenta odtwarzania jest `\shell`.  
Pliki dzienników można wyszukiwać, wybierając menu **Windows > Start**, a następnie wybierając opcje **Panel sterowania > Szukaj** i wprowadzając tekst `*.log`.

**Linux** Dzienniki są umieszczane w obu z następujących ścieżek:  
`<katalog.główny.użytkownika>/tivoli/tsm/ve/mount/log`  
`/opt/tivoli/tsm/TDPVMware/mount/engine/var`  
Pliki dziennika można wyszukiwać, wprowadzając komendę:  
`find /opt/tivoli/ -name "*.log"`

**Ważne:** Istniejące pliki dzienników są nadpisywane za każdym razem, gdy uruchamiana jest instalacja. Jeśli wystąpi problem z instalacją i trzeba będzie reinstalować produkt, należy pobrać istniejący plik `TDPVMwareInstallation.log` z katalogu `%allusersprofile%` przed ponowną próbą instalacji.

**Uwaga:** Gdy usługa Data Protection for VMware jest uruchomiona, szereg plików dzienników jest utrzymywanych w stanie otwartym. W rezultacie niektóre menedżery plików nie wyświetlają bieżącego stanu tych plików i mogą raportować ich zerową wielkość. Wybranie lub otwarcie jednego z tych plików wymusza na menedżerze plików zaktualizowanie szczegółów pliku.

## Pliki dzienników agenta odtwarzania

Plikiem dziennika agenta odtwarzania jest plik `TDP_FOR_VMWARE_MOUNTnnn.sf`. Plik dziennika zawierający najnowsze dane jest zapisany w pliku dziennika o numerze `040` (`TDP_FOR_VMWARE_MOUNT040.sf`). Po osiągnięciu przez plik dziennika limitu maksymalnej wielkości zostaje utworzony nowy plik dziennika. Nazwa pliku dziennika jest taka sama, jednak numer dziennika plików zostaje zmniejszony o jeden. Dane znajdujące się w pliku dziennika o numerze `040` są kopiowane do pliku dziennika o numerze `039`. Plik dziennika o numerze `040` zawiera najnowsze dane pliku dziennika. Gdy plik o numerze `040` ponownie osiągnie maksymalną wielkość pliku, zawartość pliku `039` zostaje przeniesiona do pliku o numerze `038`, a informacje z pliku `040` zostają ponownie przeniesione do pliku `039`.

## Pliki dzienników interfejsu GUI programu Data Protection for VMware

Interfejs GUI Data Protection for VMware vSphere umieszcza pliki dzienników w następującym katalogu:

**Windows** C:\IBM\SpectrumProtect\webserver\usr\servers\veProfile\logs

**Linux** /opt/tivoli/tsm/tdpvmware/common/webserver/usr/servers/veProfile/logs

Podczas gromadzenia plików dzienników należy pamiętać o dołączeniu wszystkich podkatalogów do skompresowanego pliku.

## Pliki dzienników interfejsu wiersza komend Data Protection for VMware

Interfejs wiersza komend Data Protection for VMware umieszcza pliki dzienników w następującym katalogu:

**Windows** C:\Program Files\IBM\SpectrumProtect\Framework\VEGUI\logs

**Linux** /opt/tivoli/tsm/tdpvmware/common/logs

Podczas gromadzenia plików dzienników należy pamiętać o dołączeniu wszystkich podkatalogów do skompresowanego pliku.

## Pliki dzienników interfejsu odtwarzania plików programu IBM Spectrum Protect

Interfejs odtwarzania plików programu IBM Spectrum Protect rejestruje komunikaty o błędach w plikach fr\_api.log, fr\_gui.log i messages.log. Pliki te znajdują się w następującym katalogu domyślnym:

**Windows** C:\IBM\SpectrumProtect\webserver\usr\servers\veProfile\logs

**Linux** /opt/tivoli/tsm/tdpvmware/common/webserver/usr/servers/veProfile/logs

Użytkownik może zmienić nazwę i lokalizację pliku fr\_api.log przez ustawienie opcji API\_LOG\_FILE\_NAME i API\_LOG\_FILE\_LOCATION w pliku aktywności dziennika odtwarzania plików (FRLog.config).

Operacje odtwarzania plików są także rejestrowane przez serwer IBM Spectrum Protect. Istnieje możliwość wyszukiwania tych komunikatów za pomocą administracyjnego klienta wiersza komend serwera.

- Aby uruchomić sesję klienta administracyjnego w trybie wiersza komend, na stacji roboczej wprowadź komendę:

```
dsmadm -id=admin -password=admin -dataonly=yes
```

Wprowadzenie komendy **DSMADM** z opcjami **-ID** i **-PASSWORD** spowoduje, że nie zostanie wyświetlone pytanie o identyfikator i hasło użytkownika.

- Aby przeszukać tabelę rozszerzonego podsumowania SQL w celu wyświetlenia wyników dotyczących operacji odtwarzania plików, w administracyjnym kliencie wiersza komend wprowadź komendę **select**:

```
select * from SUMMARY_EXTENDED where ACTIVITY_TYPE='File Restore'
```

Wyszukiwanie można zawęzić, dodając do instrukcji select jedno lub więcej spośród następujących kryteriów:

- \* ENTITY='NAZWA\_WĘZŁA\_NARZĘDZIA\_PRZENOSZENIA\_DANYCH'
- \* AS\_ENTITY='NAZWA\_WĘZŁA\_CENTRUM\_PRZETWARZANIA\_DANYCH'
- \* SUB\_ENTITY='NAZWA\_HOSTA\_VM'
- \* START\_TIME='rrrr-mm-dd gg:mm:ss'



Na przykład:

```
select * from SUMMARY_EXTENDED where ACTIVITY_TYPE='File Restore'
and ENTITY='LOCAL_MP_WIN' and AS_ENTITY='DC_NODE' and SUB_ENTITY='testvm'
and START_TIME>'2017-03-11 17:30:00'
```

Kryteria **START\_TIME** obsługują zapytania zawierające następujące znaki: znak równości (=), mniejsze od (<) lub większe od (>).

- Aby przeszukać tabelę dziennika aktywności SQL w celu wyświetlenia zdarzeń dotyczących operacji odtwarzania plików, w administracyjnym kliencie wiersza komend wprowadź komendę **select**:

```
select * from ACTLOG
```

Wyszukiwanie można zawęzić, dodając do instrukcji select jedno lub więcej spośród następujących kryteriów:

- \* **NODENAME**='NAZWA\_WĘZŁA\_CENTRUM\_PRZETWARZANIA\_DANYCH'
- \* **DATE\_TIME**='rrrr-mm-dd gg:mm:ss'

Na przykład:

```
select * from ACTLOG where NODENAME='DC_NODE' and DATE_TIME>'2017-03-11 17:30:00'
```

Wartości **NAZWA\_WĘZŁA\_CENTRUM\_PRZETWARZANIA\_DANYCH** i **NAZWA\_WĘZŁA\_CENTRUM\_PRZETWARZANIA\_DANYCH** należy podać, używając wielkich liter.

Kryteria **DATE\_TIME** obsługują zapytania zawierające następujące znaki: znak równości (=), mniejsze od (<) lub większe od (>).

---

## Uruchamianie usług dla produktu Data Protection for VMware i ich działanie

Domyślnie w momencie uruchamiania systemu operacyjnego Windows agent odtwarzania jest uruchamiany w lokalnym koncie systemowym.

### Uruchamianie agenta odtwarzania w systemie Microsoft Windows

W momencie uruchomienia agent odtwarzania za pomocą menu Start systemu Windows, usługa jest automatycznie zatrzymywana. Gdy agent odtwarzania uruchomiony za pomocą menu Start kończy działanie, usługa jest automatycznie uruchamiana. Ponadto dla tych systemów operacyjnych ta usługa nie udostępnia interfejsu GUI. Aby używać interfejsu GUI, należy przejść do menu Start systemu Windows i wybrać następujące pozycje **Wszystkie programy > IBM Spectrum Protect > Data Protection for VMware > agent odtwarzania**.

### interfejs wiersza komend Data Protection for VMware

Aby sprawdzić, czy interfejs wiersza komend Data Protection for VMware jest uruchomiony, wykonaj następujące czynności:

**Windows** Wybierz kolejno opcje **Start > Panel sterowania > Narzędzia administracyjne > Usługi** i sprawdź, czy interfejs wiersza komend Data Protection for VMware ma status Uruchomiono.

**Linux** Przejdź do katalogu scripts (/opt/tivoli/tsm/tdpvmware/common/scripts/) i wprowadź następującą komendę:  
./vmclid status

- Jeśli ten demon nie jest uruchomiony, wprowadź następującą komendę, aby ręcznie go uruchomić:

```
/opt/tivoli/tsm/tdpvmware/common/scripts/vmcli --daemon
```

Poniższych skryptów init można także używać do zatrzymywania i uruchamiania tego demona:

```
./vmclid stop
./vmclid start
```

---

## Dodatek A. Zaawansowane czynności konfiguracyjne

Należy ręcznie skonfigurować i zweryfikować każdy komponent za pomocą dostępnych interfejsów aplikacji.

### Zanim rozpoczniesz

Przed wykonaniem tego zadania należy się upewnić, że zostały spełnione następujące warunki:

- Serwer IBM Spectrum Protect musi być dostępny na potrzeby rejestrowania węzłów.
- Interfejs GUI Data Protection for VMware vSphere jest zainstalowany w systemie, który spełnia wymagania wstępne dotyczące systemu operacyjnego. Musi on mieć połączenie sieciowe z następującymi systemami:
  - Serwer vStorage Backup Server
  - Serwer IBM Spectrum Protect
  - Serwer vCenter

### Procedura

1. Zaloguj się do serwera IBM Spectrum Protect i wykonaj czynności opisane w sekcji “Konfigurowanie węzłów IBM Spectrum Protect w środowisku vSphere” na stronie 90.
2. Zaloguj się do serwera kopii zapasowych vStorage i wykonaj czynności opisane w sekcji “Konfigurowanie węzłów narzędzia przenoszenia danych w interfejsie GUI wtyczki vSphere” na stronie 91.
3. Zaloguj się do systemu, w którym jest zainstalowany interfejs GUI Data Protection for VMware vSphere, i wykonaj czynności opisane w sekcji “Konfigurowanie interfejsu wiersza komend Data Protection for VMware w środowisku vSphere” na stronie 97.
4. W systemie, w którym jest zainstalowany interfejs GUI Data Protection for VMware vSphere, uruchom klienta vSphere i zaloguj się do vCenter. Jeśli klient vSphere jest już uruchomiony, musisz go zatrzymać i zrestartować.
5. Przejdź do strony głównej klienta vSphere. Kliknij ikonę interfejsu GUI Data Protection for VMware vSphere na panelu Solutions and Applications (Rozwiązania i aplikacje).

**Wskazówka:** Jeśli ta ikona nie jest wyświetlana, oznacza to, że interfejs GUI Data Protection for VMware vSphere nie został zarejestrowany lub wystąpił błąd połączenia.

- a. W menu klienta vSphere wybierz kolejno opcje **Plug-ins (Wtyczki) > Manage Plug-ins (Zarządzaj wtyczkami)**, aby uruchomić menedżera wtyczek.
- b. Jeśli ikona interfejsu GUI Data Protection for VMware vSphere jest dostępna i wystąpił błąd połączenia, sprawdź połączenie z maszyną, na której zainstalowano interfejs GUI Data Protection for VMware vSphere, wprowadzając komendę ping.

### Wyniki

Interfejs GUI Data Protection for VMware vSphere jest gotowy do wykonywania operacji tworzenia i odtwarzania kopii zapasowych.

---

## Konfigurowanie węzłów IBM Spectrum Protect w środowisku vSphere

W tej procedurze opisano, w jaki sposób można ręcznie zarejestrować węzły na serwerze IBM Spectrum Protect i nadać uprawnienie proxy tym węzłom w środowisku vSphere.

### Zanim rozpocznieś

**Ważne:**

### O tym zadaniu

Wszystkie kroki w tej procedurze są wykonywane na serwerze IBM Spectrum Protect.

**Wskazówka:** To zadanie można także wykonać za pomocą kreatora konfiguracji interfejsu GUI Data Protection for VMware vSphere lub przez edycję notatnika konfiguracji. Uruchom interfejs GUI Data Protection for VMware vSphere, otwierając przeglądarkę WWW i przechodząc do serwera WWW interfejsu GUI. Na przykład:

<https://guihost.mycompany.com:9081/TsmVMwareUI/>

Zaloguj się, korzystając z nazwy i hasła użytkownika serwera vCenter.

- W przypadku konfiguracji początkowej wybierz opcje **Konfiguracja > Uruchom kreatora konfiguracji**.
- W przypadku konfiguracji już istniejącej wybierz opcje **Konfiguracja > Edytuj konfigurację**.

### Procedura

1. Zaloguj się do serwera IBM Spectrum Protect i uruchom w wierszu komend sesję klienta administracyjnego:  
`dsmadm -id=admin -password=admin -dataonly=yes`
2. Wprowadź komendę **REGister Node**, aby zarejestrować następujące węzły na serwerze IBM Spectrum Protect:
  - a. Węzeł, który reprezentuje VMware vCenter (węzeł vCenter):  
`REGister Node MY_VCNODE <hasło dla węzła MY_VCNODE>`
  - b. Węzeł, który zapewnia komunikację między serwerem IBM Spectrum Protect i interfejsem GUI Data Protection for VMware vSphere (węzeł VMCLI):  
`REGister Node MY_VMCLINODE <hasło dla węzła MY_VMCLINODE>`
  - c. Węzeł, który reprezentuje centrum przetwarzania danych i jest miejscem, w którym są przechowywane dane maszyny wirtualnej (węzeł centrum przetwarzania danych):  
`REGister Node MY_DCNODE <hasło dla węzła MY_DCNODE>`
  - d. Węzeł, który „przenosi dane” z jednego systemu do innego (węzeł narzędzia przenoszenia danych):  
`REGister Node MY_DMNODE <hasło dla węzła MY_DMNODE>`

**Ważne:** Podczas rejestrowania węzłów na serwerze IBM Spectrum Protect nie należy używać parametru `userid`.

3. Wprowadź komendę **GRant PROXynode**, aby zdefiniować relacje proxy dla tych węzłów:

**Zapamiętaj:** Węzły docelowe zawierają własne dane i węzły agentów działające w imieniu tych węzłów docelowych. Gdy nadano uprawnienie proxy węzłowi docelowemu, węzeł agenta może wykonywać operacje tworzenia i odtwarzania kopii zapasowych dla węzła docelowego.

- a. Nadaj uprawnienie proxy węzłowi vCenter, wprowadzając następującą komendę:  
`GRant PROXynode TArget=MY_VCNODE AGent=MY_DCNODE,MY_VMCLINODE`

Ta komenda nadaje węzłom MY\_DCNODE i MY\_VMCLINODE uprawnienie do tworzenia i odtwarzania kopii zapasowych maszyn wirtualnych w imieniu węzła MY\_VCNODE.

- b. Nadaj uprawnienie proxy węzłowi centrum przetwarzania danych, wprowadzając następującą komendę:  
`GRant PROXynode TArget=MY_DCNODE AGent=MY_VMCLINODE,MY_DMNODE`

Ta komenda nadaje węzłom MY\_VMCLINODE i MY\_DMNODE uprawnienie do tworzenia i odtwarzania kopii zapasowych maszyn wirtualnych w imieniu węzła MY\_DCNODE.

- c. (Opcjonalnie) Nadaj uprawnienie proxy dowolnym dodatkowym węzłom centrów przetwarzania danych lub węzłom narzędzia przenoszenia danych w środowisku.
- d. Sprawdź relacje proxy za pomocą komendy `Query PROXynode` serwera IBM Spectrum Protect. Oczekiwane wyjście komendy: Oczekiwane wyjście tej komendy:

| Węzeł docelowy | Węzeł agenta           |
|----------------|------------------------|
| MY_VCNODE      | MY_DCNODE MY_VMCLINODE |
| MY_DCNODE      | MY_VMCLINODE MY_DMNODE |

## Co dalej

Po pomyślnym skonfigurowaniu węzłów IBM Spectrum Protect następnym zadaniem konfiguracji ręcznej jest skonfigurowanie węzłów narzędzia przenoszenia danych, jak to opisano w sekcji “Konfigurowanie węzłów narzędzia przenoszenia danych w interfejsie GUI wtyczki vSphere”.

## Konfigurowanie węzłów narzędzia przenoszenia danych w interfejsie GUI wtyczki vSphere

Jeśli obciążenie związane z tworzeniem kopii zapasowych zostało przeniesione na serwer kopii zapasowych vStorage w środowisku vSphere, można użyć kreatora narzędzia przenoszenia danych do skonfigurowania szeregu węzłów narzędzia przenoszenia danych w celu uruchamiania operacji i przeniesienia danych na serwer IBM Spectrum Protect.

### Zanim rozpoczniesz

Konfigurowanie węzłów narzędzia przenoszenia danych wymaga zmian konfiguracji, uruchomienia niezbędnych usług i zweryfikowania instalacji.

Te zadania można wykonać za pomocą interfejsu GUI wtyczki, który upraszcza i przyspiesza tworzenie szeregu węzłów narzędzia przenoszenia danych. Alternatywnie można wykonać tę pracę samodzielnie, więcej informacji na ten temat zawiera sekcja “Ręczne konfigurowanie węzłów narzędzia przenoszenia danych w środowisku vSphere” na stronie 93.

W standardowym środowisku Data Protection for VMware dla każdego węzła narzędzia przenoszenia danych jest używany osobny plik `dsm.opt` (Windows) lub osobna sekcja w pliku `dsm.sys` (Linux). Jeśli do deduplikacji danych jest używanych wiele węzłów narzędzia przenoszenia danych na serwerze kopii zapasowych vStorage i węzły te mają uprawnienie do

przenoszenia danych dla tego samego węzła centrum przetwarzania danych, wtedy każdy plik `dsm.opt` lub każda sekcja w pliku `dsm.sys` musi zawierać inną wartość opcji `dedupcachepath`.

Zwykle fizyczny węzeł narzędzia przenoszenia danych używa sieci SAN na potrzeby operacji tworzenia i odtwarzania kopii zapasowych danych. Jeśli zostanie skonfigurowany bezpośredni dostęp węzła narzędzia przenoszenia danych do woluminów pamięci masowej, należy wyłączyć automatyczne przypisywanie liter napędów. Jeśli przypisywanie liter nie zostanie wyłączone, klient w węźle narzędzia przenoszenia danych może uszkodzić RDM (Raw Data Mapping) dysków wirtualnych. W przypadku uszkodzenia RDM dysków wirtualnych operacje tworzenia kopii zapasowych zakończą się niepowodzeniem.

**Ograniczenie:** Program Data Protection for VMware nie obsługuje tworzenia kopii zapasowych samego siebie przez serwer kopii zapasowych vStorage (który jest używany jako narzędzie przenoszenia danych). Należy upewnić się, że serwer kopii zapasowych vStorage został wykluczony z obejmujących go harmonogramów. Do utworzenia kopii zapasowej maszyny wirtualnej, która zawiera serwer kopii zapasowych vStorage, należy użyć innego serwera kopii zapasowych vStorage.

W celu przeprowadzania dowolnej z powyższych zmian, należy zapoznać się z tematem *Ręczne konfigurowanie węzłów narzędzia przenoszenia danych w środowisku vSphere*.

## O tym zadaniu

Do skonfigurowania węzłów narzędzia przenoszenia danych należy użyć wtyczki vSphere.

### Procedura

1. Z poziomu wtyczki vSphere wybierz program IBM Spectrum Protect.
2. Na karcie **Konfiguracja** wybierz opcję **Narzędzia przenoszenia danych**.
3. W panelu **Dodaj narzędzie przenoszenia danych** wybierz centrum przetwarzania danych z rozwijanego menu.
4. Zmodyfikuj odpowiednio następujące pola:
  - **Nazwa narzędzia przenoszenia danych:** nazwa węzła, wypełniona już sugerowaną nazwą złożoną z przedrostka węzła, nazwy węzła centrum przetwarzania danych, nazwy węzła narzędzia przenoszenia danych i numeru kolejnego.
  - **Nazwa hosta narzędzia przenoszenia danych**
  - **Użytkownik vCenter**, wartość już wypełniona nazwą użytkownika, który zarejestrował wtyczkę.
  - **Hasło vCenter**Kliknij opcję **Dodaj**, gdy ustawienia będą kompletne.
5. Ekran **Wyniki** zawiera następujące informacje:
  - Nazwa skonfigurowanego narzędzia przenoszenia danych.
  - Położenie pliku opcji. Edytując ten plik, można skonfigurować narzędzie przenoszenia danych.
  - Położenie plików dziennika.
  - Domyślne opcje, które zostały użyte.
6. Na karcie **IBM Spectrum Protect > Skonfiguruj narzędzia przenoszenia danych** można teraz przetestować narzędzie przenoszenia danych. Ponadto można zweryfikować instalację, wybierając narzędzie przenoszenia danych i klikając opcję **Weryfikuj** lub sprawdzając status po następnym dodaniu narzędzia przenoszenia danych.
7. Narzędzie przenoszenia danych można dodać do harmonogramu na karcie **IBM Spectrum Protect > Harmonogramy**.

## Ręczne konfigurowanie węzłów narzędzia przenoszenia danych w środowisku vSphere

Jeśli obciążenie związane z tworzeniem kopii zapasowych zostało przeniesione na serwer kopii zapasowych vStorage w środowisku vSphere, można ręcznie skonfigurować węzły narzędzia przenoszenia danych do uruchamiania operacji i przenoszenia danych na serwer IBM Spectrum Protect.

### Zanim rozpoczniesz

Zwykle fizyczny węzeł narzędzia przenoszenia danych używa sieci SAN na potrzeby operacji tworzenia i odtwarzania kopii zapasowych danych. Jeśli zostanie skonfigurowany bezpośredni dostęp węzłów narzędzia przenoszenia danych do woluminów pamięci masowej, należy wyłączyć automatyczne przypisywanie liter napędów. Jeśli przypisywanie liter nie zostanie wyłączone, klient w węźle narzędzia przenoszenia danych może uszkodzić RDM (Raw Data Mapping) dysków wirtualnych. W przypadku uszkodzenia RDM dysków wirtualnych operacje tworzenia kopii zapasowych zakończą się niepowodzeniem.

**Wymagane usługi:** Narzędzie przenoszenia danych wymaga usługi akceptora klienta, usługi agenta klienta zdalnego i usługi programu planującego narzędzia przenoszenia danych, jak to opisano w poniższych krokach. W przypadku usuwania narzędzia przenoszenia danych z centrum przetwarzania danych należy zdeinstalować i usunąć te usługi z narzędzia przenoszenia danych.

**Ważne:** Jeśli narzędzie przenoszenia danych jest zainstalowane w tym samym systemie Windows co interfejs GUI programu Data Protection for VMware vSphere i podczas konfigurowania narzędzia przenoszenia danych wybrano opcję **Utwórz usługi**, następujące kroki nie są wymagane.

W standardowym środowisku Data Protection for VMware dla każdego węzła narzędzia przenoszenia danych jest używany osobny plik `dsm.opt` (Windows) lub osobna sekcja w pliku `dsm.sys` (Linux). Jeśli do deduplikacji danych jest używanych wiele węzłów narzędzia przenoszenia danych na serwerze kopii zapasowych vStorage i węzły te mają uprawnienie do przenoszenia danych dla tego samego węzła centrum przetwarzania danych, wtedy każdy plik `dsm.opt` lub każda sekcja w pliku `dsm.sys` musi zawierać inną wartość opcji `dedupcachepath`. W celu osiągnięcia najlepszych rezultatów, należy podać inne opcje `schedlogname` i `errorlogname` dla każdego pliku `dsm.opt` lub każdej sekcji w pliku `dsm.sys`. Minimalny zestaw wymaganych opcji jest podany w kroku 2.

Zwykle fizyczny węzeł narzędzia przenoszenia danych używa sieci SAN na potrzeby operacji tworzenia i odtwarzania kopii zapasowych danych. Jeśli zostanie skonfigurowany bezpośredni dostęp węzła narzędzia przenoszenia danych do woluminów pamięci masowej, należy wyłączyć automatyczne przypisywanie liter napędów. Jeśli przypisywanie liter nie zostanie wyłączone, klient w węźle narzędzia przenoszenia danych może uszkodzić RDM (Raw Data Mapping) dysków wirtualnych. W przypadku uszkodzenia RDM dysków wirtualnych operacje tworzenia kopii zapasowych zakończą się niepowodzeniem.

**Ograniczenie:** Program Data Protection for VMware nie obsługuje tworzenia kopii zapasowych samego siebie przez serwer kopii zapasowych vStorage (który jest używany jako narzędzie przenoszenia danych). Należy upewnić się, że serwer kopii zapasowych vStorage został wykluczony z obejmujących go harmonogramów. Do utworzenia kopii zapasowej maszyny wirtualnej, która zawiera serwer kopii zapasowych vStorage, należy użyć innego serwera kopii zapasowych vStorage.

## O tym zadaniu

**Wskazówka:** Wszystkie kroki w tej procedurze są wykonywane na serwerze kopii zapasowych vStorage.

## Procedura

1. **Linux** Sprawdź, czy na komputerze docelowym jest zainstalowane oprogramowanie Java.
2. **Linux** Ustaw odpowiednie zmienne środowiskowe.
  - a. Upewnij się, że zmienna środowiskowa `JAVA_HOME` została poprawnie wyeksportowana:  
`export JAVA_HOME=<katalog_instalacyjny_środowiska_jre_lub_jdk>`
  - b. Upewnij się, że zmienna środowiskowa `PATH` została poprawnie wyeksportowana:  
`export PATH=$PATH:$JAVA_HOME/jre/bin`
  - c. Upewnij się, że zmienna środowiskowa `LD_LIBRARY_PATH` została poprawnie wyeksportowana. Sprawdź lub ustaw ją na katalog instalacyjny klienta i bibliotekę współużytkowaną Java `libjvm.so`:  
Dla środowiska IBM Java:  
`export LD_LIBRARY_PATH=/opt/tivoli/tsm/client/ba/bin:$JAVA_HOME/jre/bin/classic`  
Dla środowiska Oracle Java:  
`export LD_LIBRARY_PATH=/opt/tivoli/tsm/client/ba/bin:$JAVA_HOME/jre/lib/amd64/server`
3. Utwórz plik opcji `dsm.opt` lub `dsm.sys` w następującej lokalizacji:
  - **Windows:** `C:\Program Files\Tivoli\TSM\baclient`
  - **Linux:** `/opt/tivoli/tsm/client/ba/bin`
4. Skopiuj opcje z przykładowego pliku opcji dla narzędzia przenoszenia danych do pliku `dsm.opt` lub `dsm.sys`. Aby znaleźć przykładowy plik dla narzędzia przenoszenia danych:
  - Otwórz przeglądarkę WWW i wprowadź adres serwera WWW interfejsu GUI. Na przykład:  
`https://guihost.mycompany.com:9081/TsmVMwareUI/`
  - Zaloguj się, podając nazwę i hasło użytkownika vCenter, a następnie upewnij się, że opcja **Tryb konfiguracji** jest zaznaczona.
  - W kreatorze konfiguracji przejdź do strony Węzły narzędzia przenoszenia danych.
  - Znajdź narzędzie przenoszenia danych i kliknij opcję **Wyświetl**.
  - Skopiuj opcje przykładowe z karty **Windows** lub **Linux** do pliku opcji.

Opcje te można zaktualizować, jeśli jest to wymagane dla używanego środowiska.

Opis tych opcji znajduje się w sekcji Skorowidz opcji.

Dla operacji natychmiastowego dostępu, odtwarzania lub podłączania (odtworzenie plików) upewnij się, że do pliku opcji narzędzia przenoszenia danych dodano opcję `VMISCSISERVERADDRESS`. Podaj adres IP karty sieciowej serwera iSCSI na serwerze kopii zapasowych vStorage, który jest używany do przesyłania danych iSCSI podczas operacji natychmiastowych. Sieć fizyczna karty sieciowej (NIC), która jest podłączona do urządzenia iSCSI na hoście ESX, musi być w tej samej podsieci, co karta sieciowa na serwerze kopii zapasowych vStorage używana do przesyłania danych iSCSI.
5. Wprowadź następującą komendę, aby ustawić użytkownika i hasło VMware vCenter dla węzła narzędzia przenoszenia danych:  
`dsmc set password -type=vm vcenter.mojafirma.xyz.com <administrator> <hasło1>`
6. Skonfiguruj usługę akceptora klienta i usługę programu planującego narzędzia przenoszenia danych, wykonując następujące czynności:



- **Windows** Ta procedura wykorzystuje do skonfigurowania usługi akceptora klienta i usługi programu planującego kreator konfiguracji interfejsu GUI klienta IBM Spectrum Protect. Domyślnie za pomocą kreatora konfigurowana jest też usługa agenta zdalnego klienta. Jeśli do wykonania tego zadania używany jest program konfiguracyjny usługi klienta IBM Spectrum Protect (**dsmcutil**), należy również zainstalować usługę agenta zdalnego klienta.

Uruchom kreatora konfiguracji klienta programu IBM Spectrum Protect, wybierając z menu opcje **Narzędzia > Kreator konfiguracji**:

- Wybierz opcję **Pomóż mi skonfigurować klienta WWW TSM**. Wprowadź informacje po wyświetleniu zachęty.
  - a. W opcji Kiedy ma zostać uruchomiona usługa? wybierz **Automatycznie przy starcie Windows**.
  - b. W opcji Czy chcesz uruchomić usługę po zakończeniu tego kreatora? wybierz wartość **Tak**.

Po pomyślnym zakończeniu operacji wróć do strony powitania kreatora i przejdź do kroku b.

**Wskazówka:** Gdy na jednej maszynie konfigurujesz więcej niż jeden węzeł narzędzia przenoszenia danych, musisz podać inną wartość portu dla każdej instancji akceptora klienta.

- Wybierz opcję **Pomóż mi skonfigurować program planujący klienta TSM**. Wprowadź informacje po wyświetleniu zachęty.
  - a. Przy wprowadzaniu nazwy programu planującego zaznacz opcję **Użyj demona akceptora klienta (CAD) do zarządzania programem planującym**.
  - b. W opcji Kiedy ma zostać uruchomiona usługa? wybierz **Automatycznie przy starcie Windows**.
  - c. W opcji Czy chcesz uruchomić usługę po zakończeniu tego kreatora? wybierz wartość **Tak**.

- **Linux** Dla narzędzia przenoszenia danych w systemie Linux wykonaj następujące kroki:

- a. Program instalacyjny tworzy skrypt uruchamiający dla akceptora klienta (**dsmcad**) w katalogu **/etc/init.d**. Sprawdź lub ustaw odpowiednie zmienne środowiskowe w pliku **/etc/init.d/dsmcad**.
- b. Podaj następujące opcje w pliku **dsm.sys** w sekcji przeznaczonej dla węzła narzędzia przenoszenia danych:

– Podaj opcję **managedservices** z następującymi dwoma parametrami:  
`managedservices schedule webclient`

Powoduje to, że akceptor klienta będzie zarządzać klientem WWW i programem planującym.

- (Opcjonalnie) Jeśli informacje o harmonogramach i błędach chcesz skierować do plików dzienników innych niż domyślne, podaj opcje **schedlogname** i **errorlogname** z pełną ścieżką i nazwą pliku, w którym mają być zapisywane informacje. Na przykład:

```
schedlogname /vmsched/dsmsched_dm.log
errorlogname /vmsched/dsmerror_dm.log
```

- c. Uruchom usługę akceptora klienta:

Akceptor klienta musi zostać uruchomiony, aby mógł zarządzać zadaniami programu planującego lub klientem WWW. Jako administrator wykonaj następujące kroki:

1) Skonfiguruj usługę akceptora klienta oraz usługę programu planującego narzędzia przenoszenia danych do działania jako serwer kopii zapasowych vStorage.

2) Uruchom akceptor klienta, wprowadzając następującą komendę:

```
service dsmcad start
```

Aby włączyć automatyczne uruchamianie akceptora klienta po restarcie systemu, z poziomu zachęty powłoki dodaj usługę w następujący sposób:

```
chkconfig --add dsmcad
```

**Wskazówka:** Aby umożliwić uruchamianie komendy **dsmc** bezpośrednio w wierszu komend systemu Linux, należy także ustawić w powłoce odpowiednie zmienne środowiskowe wymienione w kroku 2.

7. Uruchom sesję wiersza komend narzędzia przenoszenia danych, korzystając z parametrów wiersza komend **-asnodename** i **-optfile**:

```
dsmc -asnodename=VC1_DC1 -optfile=dsm_DM1.opt
```

Upewnij się, że po początkowym zalogowaniu się nie jest wyświetlana zachęta do podania hasła.

**Ważne:** Aby zapobiec niepowodzeniu działania programu planującego IBM Spectrum Protect, upewnij się, że nie ustawiono opcji **asnodename** w pliku **dsm.opt** (Windows) lub w sekcji pliku **dsm.sys** (Linux). Program planujący przesyła zapytanie do serwera IBM Spectrum Protect o harmonogramy powiązane z węzłem **nodename** (węzeł narzędzia przenoszenia danych), a nie **asnodename** (węzeł centrum przetwarzania danych). Jeśli w pliku **dsm.opt** lub **dsm.sys** zostanie ustawiona opcja **asnodename**, wysyłane zapytania będą dotyczyły harmonogramów powiązanych z węzłem **asnodename** (a nie **nodename**). W wyniku tego operacja planowania nie powiedzie się. Wykonaj poniższe czynności:

a. Zweryfikuj połączenie z serwerem IBM Spectrum Protect, wprowadzając następującą komendę:

```
dsmc query session
```

Ta komenda wyświetla informacje o sesji, w tym bieżącą nazwę węzła, godzinę rozpoczęcia sesji, informacje o serwerze i połączeniu serwera.

b. Sprawdź, czy możesz utworzyć kopię zapasową maszyny wirtualnej, wprowadzając następującą komendę:

```
dsmc backup vm vm1
```

W krokach 5b i 5d **vm1** oznacza nazwę maszyny wirtualnej.

c. Sprawdź, czy operacja tworzenia kopii zapasowej została zakończona pomyślnie, wprowadzając następującą komendę:

```
dsmc query vm "*"
```

d. Sprawdź, czy maszynę wirtualną można odtworzyć, wprowadzając następującą komendę:

```
dsmc restore vm vm1 -vmname=vm1-restore
```

8. Sprawdź, czy akceptor klienta i agent są poprawnie skonfigurowane:

a. W przeglądarce WWW wpisz adres wtyczki klienta IBM Spectrum Protect vSphere. Na przykład:

```
https://guihost.mojafirma.com/vsphere-client/
```

b. Zaloguj się, używając nazwy użytkownika i hasła vCenter.

c. W kliencie WWW vSphere kliknij opcję **IBM Spectrum Protect > Configure (Skonfiguruj) > Data Movers (Narzędzia przenoszenia danych)**.

- d. Upewnij się, że dla narzędzia przenoszenia danych w kolumnie **Status** wyświetlana jest wartość **Verified (Zweryfikowano)**. Jeśli wyświetlana jest wartość **Failed (Niepowodzenie)**, umieść wskaźnik myszy nad tym statusem, aby wyświetlić komunikat dotyczący niepowodzenia.

**Wskazówka:** Jeśli zostanie zmieniony adres IP w systemie, w którym zainstalowano interfejs GUI Data Protection for VMware vSphere, należy wykonać następujące czynności:

- a. Ponownie skonfiguruj akceptor klienta, aby włączyć interfejs GUI Data Protection for VMware vSphere dla operacji. W przeciwnym razie w menedżerze wtyczek status interfejsu GUI Data Protection for VMware vSphere będzie wyświetlany jako wyłączony.

---

## Konfigurowanie interfejsu wiersza komend Data Protection for VMware w środowisku vSphere

Zaktualizuj profil interfejsu wiersza komend Data Protection for VMware w systemie, w którym zainstalowano interfejs GUI Data Protection for VMware vSphere.

### Zanim rozpoczniesz

Profil (vmcliprofile) znajduje się w następującym katalogu w systemie, w którym zainstalowano interfejs GUI Data Protection for VMware vSphere:

**Linux** /opt/tivoli/tsm/tdpvmware/common/scripts

**Windows** Wersja 64-bitowa: C:\Program Files\IBM\SpectrumProtect\Framework\VEGUI\scripts

### O tym zadaniu

Wszystkie kroki w tej procedurze są wykonywane w systemie, w którym zainstalowano interfejs GUI Data Protection for VMware vSphere.

**Wskazówka:** To zadanie można także wykonać za pomocą kreatora konfiguracji interfejsu GUI Data Protection for VMware vSphere lub za pomocą notatnika konfiguracji. Przejdź do okna Konfiguracja interfejsu GUI Data Protection for VMware vSphere i kliknij opcję **Uruchom kreatora konfiguracji** lub **Edytuj konfigurację**.

### Procedura

1. Zaktualizuj profil z użyciem następujących ustawień:

#### **VE\_TSMCLI\_NODE\_NAME**

Podaj węzeł, który łączy interfejs wiersza komend Data Protection for VMware z serwerem IBM Spectrum Protect i węzłem agenta (MY\_VMCLINODE).

**Ograniczenie:** Węzeł VMCLI nie obsługuje protokołu SSL ani uwierzytelniania LDAP podczas komunikowania się z serwerem IBM Spectrum Protect.

#### **VE\_VCENTER\_NODE\_NAME**

Podaj węzeł wirtualny, który reprezentuje vCenter (MY\_VCNODE).

#### **VE\_DATACENTER\_NAME**

Podaj węzeł wirtualny odwzorowywany na centrum przetwarzania danych.

Poprawna jest następująca składnia:

`nazwa_centrum_przetw_dan::nazwa_węzła_centrum_przetw_danych`

- W wartości `nazwa_centrum_przetwarzania_danych` rozróżniana jest wielkość liter.
- Należy pamiętać o ustawieniu tego parametru dla każdego centrum przetwarzania danych w używanym środowisku (MY\_DCNODE).
- Interfejs GUI Data Protection for VMware vSphere nie obsługuje centrów przetwarzania danych o tej samej nazwie w vCenter.

#### VE\_TSM\_SERVER\_NAME

Podaj nazwę hosta lub adres IP serwera IBM Spectrum Protect.

#### VE\_TSM\_SERVER\_PORT

Podaj port używany przez serwer IBM Spectrum Protect. Wartością domyślną jest 1500.

Poniżej podano przykładowy profil z tymi ustawieniami:

|                      |                             |
|----------------------|-----------------------------|
| VE_TSMCLI_NODE_NAME  | MY_VMCLINODE                |
| VE_VCENTER_NODE_NAME | MY_VCNODE                   |
| VE_DATACENTER_NAME   | MyDatacenter1::MY_DCNODE    |
| VE_TSM_SERVER_NAME   | tmsserver.mycompany.xyz.com |
| VE_TSM_SERVER_PORT   | 1500                        |

#### 2. Ustaw hasło węzła VMCLI w pliku `pwd.txt`.

To hasło jest przeznaczone dla węzła, który łączy interfejs wiersza komend Data Protection for VMware z serwerem IBM Spectrum Protect i węzłem narzędzia przenoszenia danych. Do jego określenia używany jest parametr profilu `VE_TSMCLI_NODE_NAME`.

##### a. Wprowadź komendę `echo`, aby utworzyć plik tekstowy, który zawiera hasło:

**Linux** `echo hasło1 > pwd.txt`

**Windows** `echo hasło1 > pwd.txt`

**Windows** Między hasłem (`hasło1`) i znakiem większości (`>`) nie może być spacji.

##### b. Wprowadź następującą komendę `vmcli`, aby ustawić hasło dla węzła VMCLI:

`vmcli -f set_password -l pwd.txt`

#### Ważne:

- **Linux** Komendę `vmcli -f set_password` należy wprowadzić jako użytkownik `tdpvmware`, a nie jako użytkownik `root`.
- **Linux** **Windows** Jeśli planowane jest generowanie raportów dotyczących ochrony aplikacji, należy podać parametr **-type VMGuest**, aby wskazać, że hasło dotyczy maszyny wirtualnej. Na przykład:

`vmcli -f set_password -type VMGuest -I password.txt`

#### 3. Sprawdź, czy interfejs wiersza komend Data Protection for VMware jest uruchomiony:

**Windows** Kliknij kolejno opcje **Start > Panel sterowania > Narzędzia administracyjne > Usługi** i sprawdź, czy interfejs wiersza komend Data Protection for VMware ma status **Uruchomiono**.

**Linux** Przejdź do katalogu `scripts (/opt/tivoli/tsm/tdpvmware/common/scripts/)` i wprowadź następującą komendę:

`./vmclid status`

- Jeśli ten demon jest uruchomiony, przejdź do kroku 4.
- Jeśli ten demon nie jest uruchomiony, wprowadź następującą komendę, aby ręcznie go uruchomić:

```
/opt/tivoli/tsm/tdpvmware/common/scripts/vmcli --daemon
```

Poniższych skryptów init można także używać do zatrzymywania i uruchamiania tego demona:

```
./vmclid stop
./vmclid start
```

4. Wprowadź poniższą komendę vmcli, aby sprawdzić, czy interfejs wiersza komend Data Protection for VMware rozpoznaje konfigurację węzła IBM Spectrum Protect:  

```
vmcli -f inquire_config -t TSM
```
5. Sprawdź poprawność węzłów, aby upewnić się, że nie wystąpiły błędy w konfiguracji:
  - a. Uruchom interfejs GUI Data Protection for VMware vSphere, klikając ikonę w oknie Solutions and Applications (Rozwiązania i aplikacje) programu vSphere Client.
  - b. Przejdź do okna Konfiguracja.
  - c. Wybierz węzeł z tabeli i kliknij opcję **Sprawdź poprawność wybranego węzła**. Informacje o statusie są wyświetlane w panelu Szczegóły statusu.

## Co dalej

Linux Windows Po pomyślnym wykonaniu trzech ręcznych czynności konfiguracyjnych opisanych w tej sekcji:

1. “Konfigurowanie węzłów IBM Spectrum Protect w środowisku vSphere” na stronie 90
2. “Konfigurowanie węzłów narzędzia przenoszenia danych w interfejsie GUI wtyczki vSphere” na stronie 91

Nie są wymagane żadne dodatkowe czynności konfiguracyjne w celu utworzenia kopii zapasowych danych maszyny wirtualnej.

---

## Lista kontrolna konfiguracji interfejsu wiersza komend środowiska vSphere

Ta procedura umożliwia skonfigurowanie programu Data Protection for VMware w środowisku vSphere za pomocą wyłącznie interfejsu wiersza komend.

### Procedura

Wykonaj krok 1 i krok 2 na serwerze IBM Spectrum Protect.

1. Zarejestruj następujące węzły na serwerze IBM Spectrum Protect:
  - a. Węzeł, który reprezentuje VMware vCenter (węzeł vCenter):  

```
REGister Node MY_VCNODE <hasło dla węzła MY_VCNODE>
```
  - b. Węzeł, który zapewnia komunikację między serwerem IBM Spectrum Protect i interfejsem GUI Data Protection for VMware vSphere (węzeł VMCLI):  

```
REGister Node MY_VMCLINODE <hasło dla węzła MY_VMCLINODE>
```
  - c. Węzeł, który reprezentuje centrum przetwarzania danych i jest miejscem, w którym są przechowywane dane maszyny wirtualnej (węzeł centrum przetwarzania danych):  

```
REGister Node MY_DCNODE <hasło dla węzła MY_DCNODE>
```
  - d. Węzeł, który „przenosi dane” z jednego systemu do innego (węzeł narzędzia przenoszenia danych):  

```
REGister Node MY_DMNODE <hasło dla węzła MY_DMNODE>
```
2. Zdefiniuj relacje proxy dla tych węzłów:
  - a. Nadaj uprawnienie proxy węzłowi vCenter, wprowadzając następującą komendę:  

```
GRant PROXynode Target=MY_VCNODE AGent=MY_DCNODE,MY_VMCLINODE
```

Ta komenda nadaje węzłom MY\_DCNODE i MY\_VMCLINODE uprawnienie do tworzenia i odtwarzania kopii zapasowych maszyn wirtualnych w imieniu węzła MY\_VCNODE.

- b. Nadaj uprawnienie proxy węzłowi centrum przetwarzania danych, wprowadzając następującą komendę:

```
GRant PROXynode TArget=MY_DCNODE AGent=MY_VMCLINODE,MY_DMNODE
```

Ta komenda nadaje węzłom MY\_VMCLINODE i MY\_DMNODE uprawnienie do tworzenia i odtwarzania kopii zapasowych maszyn wirtualnych w imieniu węzła MY\_DCNODE.

- c. (Opcjonalnie) Nadaj uprawnienie proxy dowolnym dodatkowym węzłom centrów przetwarzania danych lub węzłom narzędzia przenoszenia danych w środowisku.
- d. Sprawdź relacje proxy za pomocą komendy Query PROXynode serwera IBM Spectrum Protect. Oczekiwane wyjście komendy:

| Węzeł docelowy | Węzeł agenta           |
|----------------|------------------------|
| MY_VCNODE      | MY_DCNODE MY_VMCLINODE |
| MY_DCNODE      | MY_VMCLINODE MY_DMNODE |

Wykonaj kroki od 3 do 9 na serwerze kopii zapasowych vStorage.

3. Ustaw odpowiednie wartości dla następujących opcji narzędzia przenoszenia danych:

- Windows** Podaj następujące opcje w pliku opcji dsm.opt.
- Linux** Podaj opcje w pliku dsm.sys w sekcji przeznaczony dla węzła narzędzia przenoszenia danych.

```
NODENAME
PASSWORDACCESS
VMCHOST
VMBACKUPTYPE
MANAGEDSERVICES
TCPSERVERADDRESS
TCPPOINT
COMMMETHOD
HTTPPORT
```

**Uwaga:** Opcja HTTPPORT jest wymagana tylko w przypadku używania więcej niż jednej usługi akceptora klienta (CAD). Na przykład, jeśli istnieją dwa węzły narzędzia przenoszenia danych (i dwie usługi CAD), wtedy w pliku opcji dla każdego węzła narzędzia przenoszenia danych należy podać inną wartość HTTPPORT.

Poniżej podano przykładowy plik dsm.dm.opt z tymi opcjami:

```
NODename MY_DMNODE
PASSWORDAccess generate
VMCHost vcenter.storage.usca.example.com
VMBACKUPType Fullvm
MANAGEDServices schedule webclient
TCPServeraddress serwer_tsm.firma.com.pl
TCPPOINT 1500
COMMMethod tcpip
HTTPPORT 1583
```

4. Zweryfikuj połączenie z serwerem IBM Spectrum Protect, wprowadzając następującą komendę:
- ```
dsmc query session
```
5. Wprowadź następującą komendę, aby ustawić użytkownika i hasło VMware vCenter dla węzła narzędzia przenoszenia danych:
- ```
dsmc set password -type=vm vcenter.mojafirma.xyz.com <administrator>
<hasło1>
```

6. Skonfiguruj następujące usługi programu IBM Spectrum Protect:

- **Windows**

a. Zainstaluj usługę programu planującego:

```
dsmcutil install scheduler /name:"TSM Central Scheduler Service"
/node:MY_DMNODE /password:MY_DMNODEPWD /startnow:no /autostart:no
```

b. Zainstaluj usługę CAD:

```
dsmcutil install cad /name:"TSM CAD - MY_DMNODE" /node:MY_DMNODE
/password:MY_DMNODEPWD /optfile:c:\tsm\baclient\dsm.dm.opt
/cadschedname:"TSM Central Scheduler Service" /startnow:no /autostart:yes
```

c. Zainstaluj usługę agenta klienta zdalnego:

```
dsmcutil install remoteagent /name:"TSM AGENT" /node:MY_DMNODE
/password:MY_DMNODEPWD /optfile:c:\tsm\baclient\dsm.dm.opt
/partnername:"TSM CAD - MY_DMNODE" /startnow:no
```

- **Linux**

Podaj opcję `managedservices` w pliku `dsm.sys` w sekcji przeznaczonej dla węzła narzędzia przenoszenia danych:

Pamiętaj o podaniu parametrów `schedule` i `webclient`:

```
managedservices schedule webclient
```

Powoduje to, że akceptor klienta będzie zarządzać klientem WWW i programem planującym.

7. **Linux** Aby skonfigurować usługę akceptora klienta (CAD) i usługę programu planującego narzędzia przenoszenia danych do działania jako serwer kopii zapasowych vStorage, ustaw następującą zmienną środowiskową w pliku `/etc/init.d/dsmcad`:

```
export LD_LIBRARY_PATH=/opt/tivoli/tsm/client/ba/bin
```

8. **Linux** Uruchom usługę akceptora klienta: Program instalacyjny tworzy skrypt uruchamiający dla demona akceptora klienta (`dsmcad`) w katalogu `/etc/init.d`. Demon akceptora klienta musi zostać uruchomiony, aby mógł zarządzać zadaniami programu planującego lub klientem WWW. Jako użytkownik `root` użyj następującej komendy w celu uruchomienia demona:

```
service dsmcad start
```

Aby włączyć automatyczne uruchamianie demona akceptora klienta po restarcie systemu, z poziomu wiersza komend dodaj usługę w następujący sposób:

```
chkconfig --add dsmcad
```

9. Sprawdź, czy usługi IBM Spectrum Protect są poprawnie skonfigurowane:

a. Zaloguj się w systemie zdalnym.

b. Użyj przeglądarki do połączenia się z systemem `HOST1`, używając następującego adresu i portu:

```
http://HOST1.xyz.Twoja_firma.com:1581
```

Wykonaj krok 10 w systemie, w którym zainstalowano interfejs GUI Data Protection for VMware vSphere.

10. Ustaw odpowiednie wartości dla następujących opcji w profilu interfejsu wiersza komend Data Protection for VMware profile (`vmcliprofile`):

```
VE_TSMCLI_NODE_NAME
VE_VCENTER_NODE_NAME
VE_DATACENTER_NAME
VE_TSM_SERVER_NAME
VE_TSM_SERVER_PORT
```

Poniżej podano przykładowy profil z tymi opcjami:

|                      |                             |
|----------------------|-----------------------------|
| VE_TSMCLI_NODE_NAME  | MY_VMCLINODE                |
| VE_VCENTER_NODE_NAME | MY_VCNODE                   |
| VE_DATACENTER_NAME   | MyDatacenter1::MY_DCNODE    |
| VE_TSM_SERVER_NAME   | tsmserver.mycompany.xyz.com |
| VE_TSM_SERVER_PORT   | 1500                        |

Profil znajduje się w następujących katalogach:

**Linux** /opt/tivoli/tsm/tdpvmware/common/scripts

**Windows** Wersja 64-bitowa: C:\Program Files\IBM\SpectrumProtect\Framework\VEGUI\scripts

a. Ustaw hasło dla węzła VMCLI:

1) Wprowadź komendę echo, aby utworzyć plik tekstowy, który zawiera hasło:

**Linux**

```
echo hasł01 > pwd.txt
```

**Windows**

```
echo hasł01> pwd.txt
```

2) Wprowadź następującą komendę vmcli, aby ustawić hasło dla węzła VMCLI:

**Ważne:** **Linux** Tę komendę należy wprowadzić jako użytkownik tdpvmware, a nie jako użytkownik root.

```
vmcli -f set_password -I pwd.txt
```

b. Sprawdź, czy interfejs wiersza komend Data Protection for VMware jest uruchomiony:

**Windows**

Wprowadź następującą komendę w wierszu komend systemu Windows:  
net start

**Linux**

Wprowadź następującą komendę:  
./vmclid status

c. Wprowadź poniższą komendę vmcli, aby sprawdzić, czy interfejs wiersza komend Data Protection for VMware rozpoznaje konfigurację węzła IBM Spectrum Protect:

```
vmcli -f inquire_config -t TSM
```

## Taśmy: wytyczne dotyczące konfigurowania

Przed wykonaniem operacji tworzenia kopii zapasowej w taśmowej pamięci masowej należy zapoznać się z podanymi wytycznymi.

### Przygotowanie do operacji tworzenia kopii zapasowej na taśmach

**Linux**

**Windows**

Przed podjęciem próby utworzenia kopii zapasowej na taśmach należy ustawić następujące parametry na serwerze IBM Spectrum Protect dla kopii zapasowych tworzonych na taśmach:

1. Zdefiniuj klasę zarządzania:

```
define mgmtclass <nazwa domeny> <nazwa zestawu strategii>
 <nazwa klasy zarządzania>
```

Na przykład:

```
define mgmtclass tape tape DISK
```

2. Zdefiniuj grupę kopii:



```
define copygroup <nazwa domeny> <nazwa zestawu strategii>
 <nazwa klasy zarządzania>
destination=<nazwa puli pamięci masowej>
```

Na przykład:

```
define copygroup tape tape DISK destination=Diskpool
```

### 3. Aktywuj zestaw strategii:

```
activate policyset <nazwa domeny> <nazwa zestawu strategii>
```

Na przykład:

```
activate policyset tape tape
```

Podczas konfigurowania tworzenia kopii zapasowej na taśmach fizycznych występują dodatkowe wymagania konfiguracyjne. Metadane programu IBM Spectrum Protect (pliki kontrolne) muszą być zawsze przechowywane na dysku, a dane kopii zapasowej maszyny wirtualnej na taśmie.

- Opcja VMMC pozwala na przechowywanie kopii zapasowych VMware (i plików sterujących VMware) za pomocą innej klasy zarządzania niż domyślna klasa zarządzania.
- Opcja VMCTLMC umożliwia podanie klasy zarządzania do użycia przez pliki sterujące VMware podczas tworzenia kopii zapasowych VMware. Podana klasa zarządzania zastąpi domyślną klasę zarządzania. Zastępuje ona także klasę zarządzania określoną za pomocą opcji VMMC. Klasa zarządzania VMCTLMC musi określać pulę pamięci masowej bez migracji na taśmę.
- Opcja VMMC jest zawsze używana do sterowania czasem przechowywania kopii zapasowych maszyn wirtualnych. Ta opcja dotyczy zarówno konfiguracji z użyciem dysków, jak i taśm. Opcja VMCTLMC nie jest używana na potrzeby określania czasu przechowywania plików sterujących. Pliki sterujące i pliki danych stanowią część tej samej grupy i tracą ważność w tym samym czasie na podstawie strategii czasu przechowywania określonej dla opcji VMMC. Gdy ustawione są obie opcje, opcja VMMC jest używana dla plików danych, a opcja VMCTLMC jest używana dla plików sterujących.

**Ograniczenie:** Operacje odtwarzania wykorzystujące agenty pamięci masowej w konfiguracji bez obciążania sieci lokalnej mogą odtwarzać pliki z kopii puli pamięci masowej, pomimo że nie można pobrać danych z podstawowej puli pamięci masowej. Taka sytuacja może wystąpić, jeśli żądanie odtworzenia dotyczy konkretnego pliku lub żądanie nie używa metody bez zapytań, a podstawowa kopia pliku znajduje się w puli pamięci masowej, która nie jest dostępna w ścieżce bez obciążania sieci lokalnej. Może mieć to również wpływ na sytuacje, które nie dotyczą odtwarzania plików, takie jak operacje tworzenia kopii zapasowej Data Protection for VMware. W środowisku Data Protection for VMware zaleca się przechowywanie plików sterujących maszyną wirtualną na dysku, aby podczas odtwarzania plików z przyrostowej kopii zapasowej nie było konieczne wykonanie podłączenia. Pliki sterujące maszyny wirtualnej nie tylko powinny być umieszczone na dysku, ale również ich kopia zapasowa nie powinna znajdować się w kopii puli pamięci masowej dostępnej w ścieżce bez obciążania sieci lokalnej. Jeśli jednak pliki te znajdują się w takiej kopii, do odtworzenia plików z przyrostowej kopii zapasowej bez obciążania sieci lokalnej na kliencie Data Protection for VMware zostanie użyte podłączenie taśmy.

Jeśli środowisko serwera IBM Spectrum Protect używa migracji danych z dysków na taśmy, należy przed migracją rozważyć następujące zalecenia:

- Ustaw pulę dyskowej pamięci masowej MIGDELAY na taką wartość, która obsługuje większość żądań podłączania realizowanych z dysku. Typowe wzorce użycia wskazują, że wysoki procent indywidualnych odtworzeń plików ma miejsce w ciągu kilku dni. Na

przykład zwykle w ciągu 3 - 5 dni od czasu ostatniej modyfikacji pliku. Dlatego należy rozważyć przechowywanie danych na dysku przez ten krótki czas w celu zoptymalizowania operacji odtwarzania.

Dodatkowo, jeśli deduplikacja danych po stronie klienta używana jest z wykorzystaniem dyskowej puli pamięci masowej, należy ustawić opcję MIGDELAY na wartość uwzględniającą częste tworzenie kopii zapasowych pełnych maszyn wirtualnych. Migracja deduplikowanej puli pamięci masowej na taśmy nie powinna być wykonywana przed wykonaniem przynajmniej dwóch pełnych kopii zapasowej maszyny wirtualnej. Gdy dane zostaną przeniesione na taśmę, nie jest już dla nich wykonywana operacja deduplikowania. Na przykład, jeśli operacja deduplikowania wykonywana jest raz na tydzień, należy ustawić wartość MIGDELAY przynajmniej na 10 dni. To ustawienie zapewnia, że każda pełna kopia zapasowa identyfikuje duplikowane dane i używa tych danych z poprzedniej kopii zapasowej, zanim zostaną one przeniesione na taśmę.

- Użyj plikowej (klasa urządzeń) puli pamięci masowej zamiast dyskowej (klasa urządzeń) puli pamięci masowej. Typową wartością wielkości woluminu (określoną za pomocą parametru MAXCAPACITY klasy urządzeń) jest wartość z zakresu od 8 GB do 16 GB. Dla powiązanej puli pamięci masowej należy rozważyć użycie kolokacji według obszaru plików. Każda maszyna wirtualna, dla której tworzona jest kopia zapasowa, reprezentowana jest przez osobny obszar plików na serwerze IBM Spectrum Protect. Kolokacja według obszaru plików zapisuje dane z wielu przyrostowych kopii zapasowych danej maszyny wirtualnej na tym samym woluminie (pliku dyskowym). Podczas migrowania na taśmę funkcja kolokacji według obszaru plików oszukuje wiele przyrostowych kopii zapasowych dla danej maszyny wirtualnej i zapisuje je razem na taśmie fizycznej.

Użyj okna dialogowego **Ustawienia**, aby ustawić wartość Tryb taśmy.

Operacja tworzenia kopii zapasowej zostanie przerwana, jeśli operacja podłączenia lub natychmiastowego odtwarzania wymaga równocześnie tej samej taśmowej pamięci masowej, która jest używana przez operację tworzenia kopii zapasowej.

---

## Ręczne konfigurowanie urządzenia iSCSI w systemie Linux

### Linux

Ta procedura zawiera opis konfigurowania systemów Linux używanych podczas operacji podłączania iSCSI. Obraz stanu maszyny wirtualnej jest podłączany z pamięci masowej serwera IBM Spectrum Protect.

### Zanim rozpocznie

Podczas podłączania iSCSI obiekt docelowy iSCSI jest tworzony w systemie agenta odtwarzania. Komponent Microsoft iSCSI Initiator nie jest wymagany w systemie agenta odtwarzania.

**Wskazówka:** Program Open-iSCSI Initiator jest dostarczany z systemem Red Hat Enterprise Linux i SUSE Linux Enterprise Server.

Przed kontynuowaniem tej czynności przejrzyj następujące wymagania iSCSI:

- Z celem iSCSI można połączyć się z każdego systemu w celu utworzenia woluminu z danymi kopii zapasowej. Wolumin ten można podłączyć w innym systemie.
- Na wszystkich komputerach, które muszą się połączyć z punktem docelowym iSCSI, jest wymagany inicjator iSCSI.

- Sprawdź, czy inicjator iSCSI jest zainstalowany na komputerze z systemem, na którym mają zostać odtworzone dane.
- Jeśli wolumin obejmuje wiele dysków, musisz podłączyć wszystkie wymagane dyski. Jeśli używane są woluminy lustrzane, podłącz tylko jeden z dysków lustrzanych. Podłączenie jednego dysku zapobiega wykonaniu czasochłonnej operacji synchronizowania.

## O tym zadaniu

Wykonaj podane poniżej czynności, aby skonfigurować systemy Linux używane podczas operacji podłączania iSCSI.

## Procedura

1. Zapamiętaj nazwę inicjatora iSCSI na komputerze, na którym mają być odtworzone dane. Nazwa inicjatora iSCSI znajduje się w pliku `/etc/iscsi/initiatorname.iscsi`. Jeśli wartość `InitiatorName=` jest pusta, utwórz nazwę inicjatora za pomocą następującej komendy:  
`twauslbpoc01:~ # /sbin/iscsi-iname`

Poniżej znajduje się przykładowa nazwa inicjatora:

```
iqn.2005-03.org.open-iscsi:3f5058b1d0a0
```

2. Dodaj nazwę inicjatora do pliku `/etc/iscsi/initiatorname.iscsi`.
  - a. Zmodyfikuj plik `/etc/iscsi/initiatorname.iscsi` za pomocą edytora **vi**. Na przykład:  
`twauslbpoc01:~ # vi /etc/iscsi/initiatorname.iscsi`
  - b. Zaktualizuj parametr **InitiatorName=**, podając nazwę inicjatora. Na przykład:  
`InitiatorName=iqn.2005-03.org.open-iscsi:3f5058b1d0a0`
3. Wykonaj następujące czynności w systemie z zainstalowanym agentem odtwarzania (lub obiektem docelowym iSCSI):
  - a. Uruchom agent odtwarzania. Podaj informacje w oknach dialogowych **Wybierz serwer IBM Spectrum Protect** i **Wybierz obraz stanu**, następnie kliknij opcję **Podłącz**.
  - b. W oknie dialogowym **Wybierz miejsce podłączenia dysku docelowego** wybierz opcję **Podłącz obiekt docelowy iSCSI**.
  - c. Utwórz nazwę obiektu docelowego. Upewnij się, że jest ona unikalna i że można ją zidentyfikować z systemu, w którym działa inicjator iSCSI. Na przykład:  
`iscsi-mount-tsm4ve`
  - d. Wpisz nazwę inicjatora iSCSI zapisaną w kroku 1 i kliknij przycisk **OK**.
  - e. Sprawdź, czy właśnie podłączony wolumin jest wyświetlany w polu **Podłączone woluminy**.
4. Znajdź i uruchom program Inicjator iSCSI w systemie inicjatora wybranym w kroku 1:
  - a. Wykonaj następującą komendę, aby sprawdzić, czy usługa iSCSI jest uruchomiona:  
 Red Hat Enterprise Linux:  
`service iscsi status`

SUSE Linux Enterprise Server:

```
service open-iscsi status
```

Jeśli usługa nie jest uruchomiona, wykonaj następującą komendę, aby ją uruchomić:

Red Hat Enterprise Linux:

```
service iscsi start
```

SUSE Linux Enterprise Server:

```
service open-iscsi start
```

- b. Wykonaj następującą komendę, aby połączyć się z celem iSCSI:  
`iscsiadm -m discovery -t sendtargets -p <adres_IP/nazwa_hosta systemu agenta odtwarzania> --login`
    - c. Wykonaj następującą komendę, aby sprawdzić, czy dostępne jest nowe urządzenie surowe:  
`fdisk -l`
  5. Podłącz system plików:  
 Dla woluminu innego niż LVM wykonaj następujące komendy. W tym przykładzie nowe urządzenie to `/dev/sdb1`:  
`mkdir /katalog`  
`mount /dev/sdb1 /katalog`  
  
 Dla woluminu LVM wykonaj następujące zadania w systemie gościa z systemem Linux:
    - a. Sprawdź, czy na komputerze z systemem Linux dostępny jest skrypt `vgimportclone`. Ten skrypt nie jest dostarczany z podstawowym pakietem LVM. Może być konieczne zaktualizowanie pakietu LVM do wersji zawierającej ten skrypt.
    - b. Wyдай komendę **`vgimportclone`** i wpisz podstawową nazwę nowej grupy woluminów (`VolGroupSnap01`). Na przykład:  
`vgimportclone --basevgname /dev/VolGroupSnap01 /dev/sdb1`
    - c. Wyдай komendę **`lvchange`**, aby oznaczyć wolumin logiczny jako aktywny. Na przykład:  
`lvchange -a y /dev/VolGroupSnap01/LogVol00`
    - d. Wyдай następujące komendy, aby podłączyć wolumin:  
`mkdir /katalog`  
`mount -o ro /dev/VolGroupSnap01/LogVol00 /katalog`
  6. Po zakończeniu operacji odtwarzania plików wykonaj poniższe komendy:
    - Dla woluminu innego niż LVM wykonaj następujące komendy:
      - a. Odłącz system plików:  
`umount /dev/sdb1 /katalog`
      - b. Usuń wolumin. Jeśli wolumin jest częścią grupy woluminów, najpierw usuń wolumin z grupy woluminów, wprowadzając następującą komendę:  
`vgreduce <nazwa_grupy_woluminów> /dev/sdb1`  
  
 Następnie wyдай tę komendę, aby usunąć wolumin:  
`pvrmove /dev/sdb1`
      - c. Wyloguj się z jednego celu:  
`iscsiadm --mode node --targetname <nazwa_celu> --logout`
      - d. Wyloguj się z wielu celów:  
`iscsiadm --mode node --logout`
    - Dla woluminu LVM wykonaj następujące zadania w systemie gościa z systemem Linux:
      - a. Odłącz system plików:  
`umount /katalog`
      - b. Usuń wolumin logiczny:  
`lvm lvremove LogVol00`
      - c. Usuń grupę woluminów:  
`lvm vgremove VolGroupSnap01`
      - d. Wyloguj się z jednego celu:  
`iscsiadm --mode node --targetname <nazwa_celu> --logout`

- e. Wyloguj się z wielu celów:
- ```
iscsiadm --mode node --logout
```

Ręczne konfigurowanie urządzenia iSCSI w systemie Windows

Windows

Ta procedura zawiera opis konfigurowania systemów Windows używanych podczas operacji podłączania iSCSI. Obraz stanu jest podłączany z pamięci masowej serwera IBM Spectrum Protect.

Zanim rozpoczniesz

Przed kontynuowaniem tej czynności przejrzyj następujące wymagania iSCSI:

- Podczas podłączania iSCSI obiekt docelowy iSCSI jest tworzony w systemie agenta odtwarzania. Z celem iSCSI można połączyć się z każdego systemu w celu utworzenia woluminu z danymi kopii zapasowej. Wolumin ten można również podłączyć w innym systemie.
- Na wszystkich komputerach, które muszą się połączyć z punktem docelowym iSCSI, jest wymagany inicjator iSCSI.
- Sprawdź, czy inicjator iSCSI jest zainstalowany na komputerze z systemem, na którym mają zostać odtworzone dane.
- Komponent Microsoft iSCSI Initiator nie jest wymagany w systemie agenta odtwarzania.

Przed kontynuowaniem tej czynności przejrzyj następujące wymagania związane z dyskiem i woluminem:

- Jeśli wolumin obejmuje wiele dysków, musisz podłączyć wszystkie wymagane dyski. Jeśli używane są woluminy lustrzane, podłącz tylko jeden z dysków lustrzanych. Podłączenie jednego dysku zapobiega wykonaniu czasochłonnej operacji synchronizowania.
- Jeśli w systemie kopii zapasowych użyto wiele dysków dynamicznych, dyski te są przypisane do tej samej grupy. W związku z tym menedżer dysków systemu Windows może uważać, że brakuje niektórych dysków i wygenerować komunikat o błędzie, gdy zostanie podłączony tylko jeden dysk. Zignoruj ten komunikat. Dane na dysku, dla którego utworzono kopię zapasową, wciąż są dostępne, chyba że część danych jest na innym dysku. Ten problem można rozwiązać, podłączając wszystkie dyski dynamiczne.

O tym zadaniu

Wykonaj podane poniżej czynności, aby skonfigurować systemy Windows używane podczas operacji podłączania iSCSI.

Procedura

1. W systemie agenta odtwarzania otwórz port 3260 w zaporze firewall w sieci LAN i w kliencie Windows. Zapamiętaj nazwę inicjatora iSCSI na komputerze, na którym mają być odtworzone dane.
Nazwa inicjatora iSCSI jest wyświetlana w oknie konfiguracyjnym inicjatora iSCSI w Panelu sterowania. Na przykład:
`iqn.1991-05.com.microsoft:hostname`
2. Wykonaj następujące czynności w systemie z zainstalowanym programem agent odtwarzania (lub obiektem docelowym iSCSI):
 - a. Uruchom interfejs GUI agenta odtwarzania. Podaj informacje w oknach dialogowych. Wybierz serwer IBM Spectrum Protect i Wybierz obraz stanu, następnie kliknij opcję **Podłącz**.

- b. W oknie dialogowym Wybierz miejsce podłączenia dysku docelowego wybierz opcję **Podłącz obiekt docelowy iSCSI**.
- c. Utwórz nazwę obiektu docelowego. Upewnij się, że jest ona unikalna i że można ją zidentyfikować z systemem, w którym działa inicjator iSCSI. Na przykład:
iscsi-mount-tsm4ve
- d. Wpisz nazwę inicjatora iSCSI zapisaną w kroku 1 i kliknij przycisk **OK**.
- e. Sprawdź, czy właśnie podłączony wolumin jest wyświetlany w polu Podłączone woluminy.
- f. Jeśli agent odtwarzania jest używany w sieci iSCSI i jeśli ten agent odtwarzania nie używa narzędzia przenoszenia danych, otwórz plik C:\ProgramData\Tivoli\TSM\RecoveryAgent\mount\RecoveryAgent.conf i podaj znacznik [IMOUNT] z parametrem **Target IP** (adres docelowy):
[IMOUNT config]
Target IP=<adres IP karty sieciowej systemu,
który udostępnia cele iSCSI.>

Na przykład:

```
[General config]
param1
param2
...
[IMount config]
Target IP=9.11.153.39
```

Po dodaniu lub zmianie parametru Target IP zrestartuj interfejs GUI agenta odtwarzania lub jego interfejs wiersza komend.

3. Znajdź i uruchom program Inicjator iSCSI w systemie inicjatora wybranym w kroku 1:
 - a. Połącz się z punktem docelowym iSCSI:
 - 1) Na karcie Obiekty docelowe wpisz adres TCP/IP programu agent odtwarzania (obiektu docelowego iSCSI) używanego w kroku 2 w oknie dialogowym Obiekt docelowy. Kliknij opcję **Szybkie połączenie**.
 - 2) W oknie dialogowym Szybkie połączenie zostanie wyświetlony obiekt docelowy zgodny z nazwą obiektu docelowego określonego w kroku 2c. Jeśli jeszcze nie ma połączenia z tym obiektem docelowym, wybierz go i kliknij opcję **Połącz**.
 - b. W systemie inicjatora wybierz kolejno opcje **Panel sterowania > Narzędzia administracyjne > Zarządzanie komputerem > Magazyn > Zarządzanie dyskami**.
 - 1) Jeśli podłączony cel iSCSI jest wymieniony jako Type=Foreign, kliknij prawym przyciskiem myszy opcję **Dysk obcy** i wybierz **Importuj obce dyski**. Grupa dysków obcych jest wybrana. Kliknij przycisk **OK**.
 - 2) Na następnym ekranie wyświetlany jest typ, stan i wielkość dysku obcego. Kliknij przycisk **OK** i poczekaj na zaimportowanie dysku.
 - 3) Po zakończeniu importowania dysku naciśnij klawisz **F5** (odświeżanie). Podłączony obraz stanu iSCSI jest widoczny i ma przypisaną literę dysku. Jeśli litery dysków nie zostały automatycznie przypisane, prawym przyciskiem myszy kliknij żądaną partycję i wybierz opcję **Zmień litery lub ścieżki dysków**. Kliknij przycisk **Dodaj** i wybierz literę dysku.
4. Otwórz Eksplorator Windows (lub inny program narzędziowy) i przeglądaj podłączony obraz stanu w celu wykonania operacji odtwarzania plików.
5. Po zakończeniu odtwarzania wykonaj następujące czynności:
 - a. Rozłącz każdy cel iSCSI, używając okna dialogowego Właściwości inicjatora iSCSI.
 - b. Odłącz wolumin podłączony w kroku 2, wybierając go w interfejsie agenta odtwarzania i klikając przycisk **Odłącz**.

Ręczne konfigurowanie węzłów proxy podłączania w systemie Linux

Linux

Wykonaj to zadanie, aby dodać węzeł proxy podłączania w zdalnym systemie Linux.

Zanim rozpocznieś

W standardowym środowisku interfejsu GUI Data Protection for VMware vSphere używana jest osobna sekcja w pliku `dsm.sys` dla każdego węzła proxy podłączania. Wszystkie kroki podane w tej procedurze wykonuje się za pomocą narzędzia przenoszenia danych zainstalowanego na serwerze kopii zapasowych.

O tym zadaniu

W tym zadaniu konfigurowane są węzły proxy podłączania przez zaktualizowanie opcji narzędzia przenoszenia danych i sprawdzenie łączności z serwerem IBM Spectrum Protect.

Procedura

1. Podaj opcje w pliku `dsm.sys` w sekcji przeznaczonej dla węzła proxy podłączania.

NODENAME

Podaj nazwę wcześniej zdefiniowanego węzła proxy podłączania.
Harmonogramy IBM Spectrum Protect są powiązane z tym węzłem.

PASSWORDACCESS

Podaj wartość `GENERATE`, aby hasło było generowane automatycznie (zamiast wyświetlania zachęty dla użytkownika).

MANAGEDSERVICES

Podaj tę opcję, aby kierować akceptor klienta do zarządzania zarówno klientem WWW, jak i programem planującym (`schedule webclient`).

TCPSERVERADDRESS

Podaj adres TCP/IP dla serwera IBM Spectrum Protect.

TCPPORT

Podaj adres portu protokołu TCP/IP dla serwera IBM Spectrum Protect.

COMMMETHOD

Podaj metodę komunikacji używaną przez serwer IBM Spectrum Protect. Dla węzłów proxy podłączania musisz podać TCP/IP jako metodę komunikacji. Jeśli zostanie podana inna metoda, operacja nie powiedzie się.

HTTPPORT

W tej opcji jest określony adres portu TCP/IP i jest ona wymagana tylko w przypadku używania więcej niż jednej usługi akceptora klienta (CAD). Na przykład, jeśli istnieją dwa węzły proxy podłączania (i dwie usługi CAD), wtedy w pliku opcji dla każdego węzła proxy podłączania należy podać inną wartość `HTTPPORT`.

Ograniczenie: Nie należy włączać opcji trybu bez obciążania sieci LAN (`ENABLELANFREE YES`) w pliku `dsm.sys`. Ta opcja nie jest obsługiwana dla węzłów proxy podłączania.

Poniżej podano przykładowy plik `dsm.sys` z tymi ustawieniami:

```
Servename      tsm_server1
NODename       datacenter1_MP_LNX
PASSWORDAccess generate
MANAGEDServices schedule webclient
```

```
TCPServeraddress tsmserver.myco.com
TCPPort          1500
COMMMethod tcpip
HTTPPORT 1583
```

2. Wprowadź następującą komendę, aby ustawić użytkownika i hasło VMware vCenter dla węzła proxy podłączania:
`dsmc set password -type=vm vcenter.mojafirma.xyz.com <administrator>
<hasło1>`
3. Uruchom sesję wiersza komend narzędzia przenoszenia danych, korzystając z parametrów wiersza komend `-asnodename` i `-optfile`:
`dsmc -asnodename=vctr1_datacenter1 -optfile=dsm_MP_LNX.sys`
Upewnij się, że po początkowym zalogowaniu się nie jest wyświetlana zachęta do podania hasła.

Ważne: Aby zapobiec niepowodzeniu działania programu planującego IBM Spectrum Protect, upewnij się, że nie ustawiono opcji `asnodename` w sekcji pliku `dsm.sys` (Linux). Program planujący przesyła zapytanie do serwera IBM Spectrum Protect o harmonogramy powiązane z węzłem `nodename` (węzeł proxy podłączania), a nie `asnodename` (węzeł centrum przetwarzania danych). Jeśli w pliku `dsm.sys` zostanie ustawiona opcja `asnodename`, wysyłane zapytania będą dotyczyć harmonogramów powiązanych z węzłem `asnodename` (a nie `nodename`). W wyniku tego operacja planowania nie powiedzie się.

4. Zweryfikuj połączenie z serwerem IBM Spectrum Protect, wprowadzając następującą komendę:

```
dsmc query session
```

Ta komenda wyświetla informacje o sesji, w tym bieżącą nazwę węzła, godzinę rozpoczęcia sesji, informacje o serwerze i połączeniu serwera.

5. Skonfiguruj usługę akceptora klienta (CAD) i usługę programu planującego narzędzia przenoszenia danych, wykonując następujące czynności:

- Podaj opcje w pliku `dsm.sys` w sekcji przeznaczonej dla węzła proxy podłączania:
 - Podaj opcję `managedservices` z następującymi dwoma parametrami:
`managedservices schedule webclient`

Powoduje to, że akceptor klienta będzie zarządzać klientem WWW i programem planującym.

- Jeśli chcesz przekierować informacje o planowaniu i błędach do plików dzienników innych, niż domyślne, podaj opcje `schedlogname` i `errorlogname`. Każda opcja musi zawierać pełną ścieżkę i nazwę pliku, w którym mają być przechowywane informacje dziennika. Na przykład:

```
schedlogname /vmsched/dsmsched_mp_lnx.log
errorlogname /vmsched/dsmerror_mp_lnx.log
```

- Aby skonfigurować usługę akceptora klienta (CAD) i usługę programu planującego narzędzia przenoszenia danych do działania jako serwer kopii zapasowych, ustaw następującą zmienną środowiskową w pliku `/etc/init.d/dsmcad`:

```
export LD_LIBRARY_PATH=/opt/tivoli/tsm/client/ba/bin
```

- Uruchom usługę akceptora klienta:

Program instalacyjny tworzy skrypt uruchamiający dla demona akceptora klienta (`dsmcad`) w katalogu `/etc/init.d`. Demon akceptora klienta musi zostać uruchomiony, aby mógł zarządzać zadaniami programu planującego lub klientem WWW. Jako użytkownik root użyj następującej komendy w celu uruchomienia demona:

```
export LD_LIBRARY_PATH=/opt/tivoli/tsm/client/ba/bin
service dsmcad start
```


Aby włączyć automatyczne uruchamianie demona akceptora klienta po restarcie systemu, z poziomu wiersza komend dodaj usługę w następujący sposób:

```
# chkconfig --add dsmcad
```

6. Sprawdź, czy akceptor klienta i agent są poprawnie skonfigurowane:
 - a. Zaloguj się w systemie zdalnym.
 - b. Użyj przeglądarki do połączenia się z systemem HOST1, używając następującego adresu i portu:
`http://HOST1.xyz.Twoja_firma.com:1581`

Ręczne konfigurowanie węzłów proxy podłączania w zdalnym systemie Windows

Windows

Wykonaj to zadanie, aby dodać węzeł proxy podłączania w zdalnym systemie Windows. To zadanie jest wymagane, jeśli chcesz dodać drugi węzeł proxy podłączania Windows w używanym środowisku.

Zanim rozpocznieś

Przed kontynuowaniem tej czynności upewnij się, że skonfigurowany jest podstawowy węzeł proxy podłączania Windows.

O tym zadaniu

Wykonaj następujące czynności w zdalnym systemie proxy podłączania Windows:

Procedura

1. W zdalnym systemie proxy podłączania Windows zainstaluj następujące produkty:
 - agent odtwarzania
 - narzędzie przenoszenia danych IBM Spectrum Protect

Oba te produkty są dostępne w pobranym obrazie programu IBM Spectrum Protect for Virtual Environments. Szczegółowe instrukcje instalacji zostały opisane w Centrum wiedzy IBM w sekcji “Instalowanie komponentów programu Data Protection for VMware w systemach Windows” na stronie 23
2. Pobierz zawartość przykładowego pliku opcji z utworzonego węzła proxy podłączania Windows i dodaj ją do pliku opcji w zdalnym systemie proxy podłączania Windows:
 - a. W podstawowym systemie proxy podłączania Windows przejdź do okna Konfiguracja w interfejsie GUI Data Protection for VMware vSphere.
 - b. Kliknij pozycję **Edytuj konfigurację TSM** na liście Zadania. Załadowanie notatnika konfiguracji może chwilę potrwać.
 - c. Przejdź do strony Pary węzłów proxy podłączania.
 - d. W kolumnie Węzeł podstawowy tabeli przejdź do węzła proxy podłączania Windows z oczekującą lokalizacją i kliknij przycisk **Wyświetl ustawienia**.
 - e. Skopiuj zawartość przykładowego pliku `dsm.opt` wyświetlanego w oknie dialogowym **Ustawienia proxy podłączania**.
 - f. Wklej (lub przepisz) zawartość przykładowego pliku `dsm.opt` do pliku opcji w zdalnym systemie proxy podłączania Windows. Nazwij plik opcji, tak aby można było go łatwo zidentyfikować jako zdalny węzeł proxy podłączania.
Na przykład: `dsm.ZDALNY1_MP_WIN.opt`.

Ograniczenie: Nie należy włączać opcji trybu bez obciążania sieci LAN (ENABLELANFREE YES) w pliku opcji. Ta opcja nie jest obsługiwana dla węzłów proxy podłączania.

3. Wprowadź następującą komendę narzędzia przenoszenia danych, aby ustawić użytkownika i hasło VMware vCenter dla węzła proxy podłączania:

Wskazówka: Aby wydać komendę dsmc, otwórz menu **Windows Start** i kliknij **Programy > IBM Spectrum Protect > Interfejs wiersza komend klienta kopii zapasowych**.

```
dsmc set password -type=vm vcenter.mojafirma.xyz.com <administrator> <hasło1>
-optfile=dsm.ZDALNY1_MP_WIN.opt
```

4. Zweryfikuj połączenie z serwerem IBM Spectrum Protect, wprowadzając następującą komendę:

```
dsmc query session -optfile=dsm.ZDALNY1_MP_WIN.opt
```

Ta komenda wyświetla informacje o sesji, w tym bieżącą nazwę węzła, godzinę rozpoczęcia sesji, informacje o serwerze i połączeniu serwera.

5. Skonfiguruj usługę akceptora klienta (CAD) i usługę programu planującego narzędzia przenoszenia danych, wykonując następujące kroki:
Ta procedura wykorzystuje do skonfigurowania usługi CAD i usługi programu planującego kreator konfiguracji interfejsu graficznego klienta IBM Spectrum Protect. Domyślnie za pomocą kreatora konfigurowana jest też usługa agenta zdalnego klienta. Jeśli do wykonania tego zadania używany jest program konfiguracyjny usługi klienta IBM Spectrum Protect (dsmcutil), należy również zainstalować usługę agenta zdalnego klienta.

Uruchom kreatora konfiguracji klienta programu IBM Spectrum Protect, wybierając z menu opcje **Narzędzia > Kreator konfiguracji**:

- a. Wybierz opcję Pomóż mi skonfigurować klienta WWW TSM. Wprowadź informacje po wyświetleniu zachęty.
 - 1) W opcji Kiedy ma zostać uruchomiona usługa? wybierz Automatycznie przy starcie Windows.
 - 2) W opcji Czy chcesz uruchomić usługę po zakończeniu tego kreatora? wybierz wartość Tak.

Po pomyślnym zakończeniu operacji wróć do strony powitania kreatora i przejdź do kroku b.

Wskazówka: Gdy w jednym systemie konfigurujesz więcej niż jeden węzeł proxy podłączania, musisz podać inną wartość portu dla każdej instancji akceptora klienta.

- b. Wybierz opcję Pomóż mi skonfigurować program planujący klienta TSM. Wprowadź informacje po wyświetleniu zachęty.
 - 1) Przy wprowadzaniu nazwy programu planującego zaznacz opcję Użyj demona akceptora klienta (CAD) do zarządzania programem planującym.
 - 2) W opcji Kiedy ma zostać uruchomiona usługa? wybierz Automatycznie przy starcie Windows.
 - 3) W opcji Czy chcesz uruchomić usługę po zakończeniu tego kreatora? wybierz wartość Tak.

6. Sprawdź, czy akceptor klienta i agent są poprawnie skonfigurowane. Użyj przeglądarki do połączenia się z systemem HOST1, używając następującego adresu i portu:

http://HOST1.xyz.Twoja_firma.com:1581

Ręczne konfigurowanie wielu akceptorów klienta w systemie Linux

W pewnych okolicznościach może być korzystne użycie wielu usług dsmcad na hoście klienta Linux.

O tym zadaniu

To zadanie skonfiguruje wiele instancji dsmcad, które będą automatycznie uruchamiane podczas startu systemu:

Procedura

1. Utwórz dwie unikalne sekcje węzła w pliku dsm.sys (domyślnie znajduje się on w katalogu /opt/tivoli/tsm/client/ba/bin/):

```
# cat /opt/tivoli/tsm/client/ba/bin/dsm.sys
SErvername node1
COMMMethod      TCPip
TCPPort         1500
TCPServeraddress localhost
nodename        node1
errorlogname     /opt/tivoli/tsm/client/ba/bin/dsmerror-node1.log
schedlogname     /opt/tivoli/tsm/client/ba/bin/dsmsched-node1.log
managedservices  webclient sched
httpport        1581
passwordaccess   generate

SErvername node2
COMMMethod      TCPip
TCPPort         1500
TCPServeraddress localhost
nodename        node2
errorlogname     /opt/tivoli/tsm/client/ba/bin/dsmerror-node2.log
schedlogname     /opt/tivoli/tsm/client/ba/bin/dsmsched-node2.log
managedservices  webclient sched
httpport        1582
passwordaccess   generate
```

Wskazówka: Może być korzystne dołączenie niektórych opcji includes/exclude w celu rozróżnienia tych węzłów. W przeciwnym razie te same dane mogą zostać uwzględnione w kopiach zapasowych z użycie dwóch nazw węzłów.

2. Utwórz dwa pliki dsm.opt, po jednym pliku dla każdego węzła (domyślnie te pliki znajdują się w katalogu /opt/tivoli/tsm/client/ba/bin/):

```
# cat /opt/tivoli/tsm/client/ba/bin/dsm-node1.opt
servername node1
# cat /opt/tivoli/tsm/client/ba/bin/dsm-node2.opt
servername node2
```

3. Włącz opcję passwordaccess generate, logując się za pomocą informacji autoryzacyjnych dla obu węzłów:

```
# cat /opt/tivoli/tsm/client/ba/bin/dsm-node1.opt
servername node1
# cat /opt/tivoli/tsm/client/ba/bin/dsm-node2.opt
servername node2
```

4. Utwórz dwie kopie domyślnego skryptu inicjującego rc.dsmcad (domyślnie ten skrypt znajduje się w katalogu /opt/tivoli/tsm/client/ba/bin/):

```
# cp /opt/tivoli/tsm/client/ba/bin/rc.dsmcad /opt/tivoli/tsm/client/ba/bin/rc.dsmcad-node1
# cp /opt/tivoli/tsm/client/ba/bin/rc.dsmcad /opt/tivoli/tsm/client/ba/bin/rc.dsmcad-node2
```

5. Zmodyfikuj plik rc.dsmcad-node1:

- a. Zmień ten wiersz dla dystrybucji Red Hat Enterprise Linux:

```
daemon $DSMCAD_BIN
```

Na ten wiersz:

```
daemon $DSMCAD_BIN -optfile=/opt/tivoli/tsm/client/ba/bin/dsm-node1.opt
```

- b. Zmień ten wiersz dla dystrybucji SUSE Linux Enterprise Server:

```
startproc $DSMCAD_BIN
```

Na ten wiersz:

```
startproc $DSMCAD_BIN -optfile=/opt/tivoli/tsm/client/ba/bin/dsm-node1.opt
```

6. Zmodyfikuj plik rc.dsmcad-node2:

- a. Zmień ten wiersz dla dystrybucji Red Hat Enterprise Linux:

```
daemon $DSMCAD_BIN
```

Na ten wiersz:

```
daemon $DSMCAD_BIN -optfile=/opt/tivoli/tsm/client/ba/bin/dsm-node2.opt
```

- b. Zmień ten wiersz dla dystrybucji SUSE Linux Enterprise Server:

```
startproc $DSMCAD_BIN
```

Na ten wiersz:

```
startproc $DSMCAD_BIN -optfile=/opt/tivoli/tsm/client/ba/bin/dsm-node2.opt
```

7. Utwórz nowe dowiązania w katalogu `/etc/init.d/`, aby wskazać dwa nowe skrypty inicjacyjne rc.dsmcad. Te dowiązania umożliwiają usłudze init w systemie Linux uruchomienie usług dsmcad podczas startu systemu:

```
# ln -s /opt/tivoli/tsm/client/ba/bin/rc.dsmcad-node2 dsmcad-node2
# ln -s /opt/tivoli/tsm/client/ba/bin/rc.dsmcad-node1 dsmcad-node1
# ls -la dsm*
lrwxrwxrwx. 1 root root 45 Aug  2 08:04 dsmcad-node1 -> /opt/tivoli/tsm/client/ba/bin/rc.dsmcad-node1
lrwxrwxrwx. 1 root root 45 Aug  2 08:04 dsmcad-node2 -> /opt/tivoli/tsm/client/ba/bin/rc.dsmcad-node2
```

8. Zarejestruj dwa nowe skrypty rc za pomocą komendy **chkconfig**:

```
# chkconfig --add dsmcad-node1
# chkconfig --add dsmcad-node2
```

9. Przetestuj konfigurację za pomocą komendy **service dsmcad start**, aby sprawdzić, czy skrypty ładują i wykonują się bez problemów:

```
# service dsmcad-node1 start
Starting dsmcad-node1: [ OK ]
# service dsmcad-node2 start
Starting dsmcad-node2: [ OK ]
# ps -ef | grep dsmcad
root 2689 1 0 09:04 ? 00:00:00 /opt/tivoli/tsm/client/ba/bin/dsmcad
-optfile=/opt/tivoli/tsm/client/ba/bin/dsm-node1.opt
root 2719 1 0 09:04 ? 00:00:00 /opt/tivoli/tsm/client/ba/bin/dsmcad
-optfile=/opt/tivoli/tsm/client/ba/bin/dsm-node2.opt
```

W tym przykładzie tekst komendy jest podzielony na dwa wiersze, aby dostosować komendę do formatu strony.

10. Zrestartuj system i sprawdź, czy dwie instancje usługi dsmcad zostały automatycznie uruchomione:

```
# ps -ef | grep dsmcad
root 1830 1 0 09:14 ? 00:00:00 /opt/tivoli/tsm/client/ba/bin/dsmcad
-optfile=/opt/tivoli/tsm/client/ba/bin/dsm-node1.opt
root 1856 1 0 09:14 ? 00:00:00 /opt/tivoli/tsm/client/ba/bin/dsmcad
-optfile=/opt/tivoli/tsm/client/ba/bin/dsm-node2.opt
```

W tym przykładzie tekst komendy jest podzielony na dwa wiersze, aby dostosować komendę do formatu strony.

Modyfikowanie pliku konfiguracyjnego interfejsu VMCLI

Plik konfiguracyjny interfejsu VMCLI (vmcliConfiguration.xml) zawiera ustawienia interfejsu GUI Data Protection for VMware vSphere.

Proces instalowania programu Data Protection for VMware wymaga, aby użytkownik podał adres IP serwera vCenter, a także określił, czy włączyć dostęp do interfejsu GUI przez przeglądarkę WWW. Po instalacji instalator nie może modyfikować adresu IP serwera ani metody dostępu do interfejsu GUI.

Aby zaktualizować te ustawienia, można ręcznie zmodyfikować plik konfiguracyjny interfejsu VMCLI (vmcliConfiguration.xml). Ten plik jest tworzony podczas instalacji w następujących lokalizacjach:

W systemach Windows:

C:\IBM\SpectrumProtect\webserver\usr\servers\veProfile\tsmVmGUI

W systemach Linux:

/opt/tivoli/tsm/tdpvmware/common/webserver/usr/servers/veProfile/tsmVmGUI/

Aby zmodyfikować ustawienie określające, czy włączyć dostęp do interfejsu GUI przez przeglądarkę WWW, wprowadź jedną z następujących wartości w parametrze

<enable_direct_start></enable_direct_start>:

- **yes**: dostęp do interfejsu GUI jest możliwy bezpośrednio za pomocą przeglądarki WWW.
Na przykład:

```
<enable_direct_start>yes</enable_direct_start>
```

- **no**: dostęp do interfejsu GUI jest niemożliwy bezpośrednio za pomocą przeglądarki WWW.
Na przykład:

```
<enable_direct_start>no</enable_direct_start>
```

Aby używać interfejsu GUI na potrzeby ochrony środowiska vSphere, w parametrze **<mode></mode>** należy podać następującą wartość:

- *vcenter*: interfejs GUI jest używany na potrzeby ochrony środowiska vSphere. Na przykład:

```
<mode>vcenter</mode>
```

Aby zmodyfikować adres IP serwera vCenter, należy się upewnić, że ustawiono parametr **<mode>vcenter</mode>**, a następnie należy podać adres IP za pomocą parametru **<vcenter_url></vcenter_url>**. Na przykład:

```
<vcenter_url>https://vcenter.myco.com/sdk</vcenter_url>
```

Na początku adresu IP serwera vCenter wymagane jest podanie wartości **https://**. Na końcu adresu IP serwera vCenter wymagane jest podanie wartości **/sdk**.

Przykładowe pliki vmcliConfiguration.xml

Następujący plik vmcliConfiguration.xml jest skonfigurowany do ochrony środowiska vSphere, a dostęp do interfejsu GUI przez przeglądarkę WWW jest włączony:

```
<?xml version="1.0" encoding="UTF-8"?>
<vmcliAdaptor>
  <VMCLIPath>C:\Program Files\IBM\SpectrumProtect\Framework\VEGUI\scripts\
</VMCLIPath>
  <interruptDelay>900000</interruptDelay>
  <mode>vcenter</mode>
  <vcenter_url>https://vcenter.myco.com/sdk</vcenter_url>
  <enable_direct_start>yes</enable_direct_start>
</vmcliAdaptor>
```

Dodatek B. Migrowanie do strategii kopii zapasowej typu zawsze przyrostowa - przyrostowa

Ta procedura służy do przeprowadzenia migracji istniejących harmonogramów tworzenia kopii zapasowych, strategii i węzłów narzędzia przenoszenia danych do użycia w strategii kopii zapasowej typu zawsze przyrostowa.

Zanim rozpoczniesz

Można użyć strategii kopii zapasowej typu zawsze przyrostowa - pełna, która została zaimplementowana w programie Data Protection for VMware w wersjach 6.2 i 6.3. Aby kontynuować korzystanie ze strategii kopii zapasowej typu zawsze przyrostowa - pełna, nie trzeba zmieniać strategii lub harmonogramów. Należy tylko dopilnować aktualizacji węzłów narzędzia przenoszenia danych do wersji 6.4 (lub nowszej) zgodnie z opisem w poniższej procedurze. Aby jednak używać strategii kopii zapasowej typu zawsze przyrostowa - przyrostowa, oprócz aktualizacji węzłów narzędzia przenoszenia danych do wersji 6.4 (lub nowszej), należy także zaktualizować harmonogramy i strategię dla tych węzłów narzędzia przenoszenia danych, które są przenoszone do tej strategii kopii zapasowej typu zawsze przyrostowa - przyrostowa.

Aby przeprowadzić migrację istniejących harmonogramów programu Data Protection for VMware do strategii kopii zapasowej typu zawsze przyrostowa - przyrostowa, należy wykonać czynności opisane w tej procedurze.

Ważne:

- Choć niektóre czynności są odrębne, wszystkie aplikacje i komponenty muszą zostać ostatecznie zaktualizowane w celu pełnego wykorzystania strategii typu zawsze przyrostowa - przyrostowa. Ta publikacja zawiera wszystkie informacje niezbędne dla każdej czynności.
- Istnieje kilka metod umożliwiających zakończenie całego procesu migrowania. Jednak to metody opisane w tej publikacji uważa się za wydajne metody w przypadku typowych środowisk programu Data Protection for VMware.
- Harmonogram, który zostanie zmigrowany w ramach tej procedury, został utworzony za pomocą kreatora tworzenia kopii zapasowych dostępnego w interfejsie GUI Data Protection for VMware vSphere. Jeśli harmonogram, który ma zostać zmigrowany, został utworzony ręcznie, aktualizacje harmonogramu podane w tej procedurze muszą być wykonywane ręcznie.

O tym zadaniu

Procedura

1. Przeprowadź aktualizację wszystkich serwerów kopii zapasowych vStorage chroniących pojedynczy serwer vCenter. Zadbaj o to, aby ta aktualizacja została jednocześnie zakończona dla wszystkich węzłów narzędzia przenoszenia danych.
 - Ta aktualizacja wymaga zainstalowania narzędzia przenoszenia danych programu IBM Spectrum Protect w wersji 6.4 (lub nowszej) na serwerze kopii zapasowych vStorage.
 - Ze względu na odrębność zadania, nie trzeba wykonać kroku 2 ani kroku 3 bezpośrednio po kroku 1. Po zaktualizowaniu węzłów narzędzia przenoszenia danych można kontynuować tworzenie kopii zapasowych maszyn wirtualnych w istniejącym środowisku. Kroki 2 i 3 można wykonać w dogodniejszym momencie.

Wskazówka: Jeśli w środowisku używanych jest wiele serwerów kopii zapasowych vStorage, można rozważyć zaktualizowanie tylko jednego serwera. Następnie należy sprawdzić, czy ten serwer działa poprawnie przed aktualizacją pozostałych serwerów kopii zapasowych vStorage.

2. Zaktualizuj strategię kopii zapasowych i harmonogramy tworzenia kopii zapasowych w celu zaimplementowania kopii zapasowych typu zawsze przyrostowa - przyrostowa: Wykonaj następujące zadania dotyczące strategii kopii zapasowej na serwerze IBM Spectrum Protect, wprowadzając komendy w kliencie komend administracyjnych (dsmadm):
 - a. Utwórz klasę zarządzania dla odpowiedniej domeny i zestawu strategii dla kopii zapasowych typu zawsze przyrostowa - przyrostowa. W podanym przykładzie tworzona jest klasa zarządzania `mgmt_ifincr28` dla domeny `domain1` i zestawu strategii `prodbackups`. Nazwa klasy zarządzania została użyta do opisania strategii kopii zapasowej typu zawsze przyrostowa - przyrostowa (ifincr — incremental-forever incremental), w której przechowywanych jest 28 wersji kopii zapasowych:

```
define mgmtclass domain1 prodbackups mgmt_ifincr28
description="Przechowywanie 28 wersji kopii zapasowych"
```
 - b. Utwórz grupę kopii zapasowych dla kopii zapasowych typu zawsze przyrostowa - przyrostowa. W tym przykładzie tworzona jest standardowa grupa kopii zapasowych dla domeny `domain1`, zestawu strategii `prodbackups` i klasy zarządzania `mgmt_ifincr28`:

```
define copygroup domain1 prodbackups mgmt_ifincr28 standard type=backup
```

Pozycje `standard type=backup` są wartościami domyślnymi i nie muszą być podane. Zostały one umieszczone w tym przykładzie, aby pokazać, że nazwą grupy kopii jest `STANDARD`, a typem grupy kopii jest `backup` (zamiast `archive`).
 - c. Zaktualizuj grupę kopii zapasowych z użyciem odpowiednich ustawień wersji, czasu przechowywania i utraty ważności:

Zapamiętaj: W programie Data Protection for VMware w wersjach 6.2 i 6.3 wersje kopii zapasowych, czasy przechowywania i utrata ważności są oparte na poziomie granulacji łańcucha kopii zapasowej. Ta metoda oznacza, że nawet wtedy, gdy tworzone są kopie zapasowe typu zawsze przyrostowa - pełna i zawsze przyrostowa - przyrostowa (w ramach strategii kopii zapasowej typu zawsze przyrostowa - pełna w wersjach 6.2 i 6.3), na potrzeby zliczania dla utraty ważności uwzględniane są tylko pełne kopie zapasowe. W programie Data Protection for VMware w wersji 6.4 wersje kopii zapasowych, czasy przechowywania i utrata ważności są oparte na poziomie granulacji pojedynczej kopii zapasowej. W tej metodzie na potrzeby zliczania dla utraty ważności uwzględniane są zarówno kopie zapasowe typu zawsze przyrostowa - pełna, jak i typu zawsze przyrostowa - przyrostowa.

Parametr `verexists` określa maksymalną liczbę wersji kopii zapasowych przechowywanych na serwerze. Jeśli operacja tworzenia kopii zapasowej typu zawsze przyrostowa - przyrostowa spowoduje przekroczenie tej liczby, serwer spowoduje utratę ważności najstarszej wersji kopii zapasowej, która istnieje w pamięci masowej serwera. W tym przykładzie określono `verexists=28`. Ta wartość oznacza, że na serwerze przechowywanych jest maksymalnie 28 wersji kopii zapasowych.

Parametr `retextra` określa maksymalną liczbę dni przechowywania wersji kopii zapasowej po tym, gdy ta wersja stanie się nieaktywna. W tym przykładzie określono `retextra=nolimit`. Ta wartość oznacza, że maksymalna liczba nieaktywnych wersji kopii zapasowych maszyn wirtualnych jest przechowywana bezterminowo. Jeśli jednak określono parametr `verexists`, wartość `nolimit` jest zastępowana wartością

parametru **verexists**. W wyniku tego w tym przykładzie maksymalnie 28 nieaktywnych wersji kopii zapasowych maszyn wirtualnych jest przechowywanych na serwerze.

Na podstawie ustawień opisanych w tym kroku, grupa kopii zapasowych jest aktualizowana w następujący sposób:

```
update copygroup domain1 prodbackups mgmt_ifincr28 verexists=28  
retextra=nolimit
```

W tym przykładzie istniejące środowisko programu Data Protection for VMware w wersji 6.3 składa się z następujących hostów i harmonogramów:

- Klaster ESX (**esxcluster**), który zawiera dwa hosty ESX (**esxhost1** i **esxhost2**).
- Harmonogram **bup_esxcluster_full** co tydzień uruchamia tworzenie kopii zapasowej typu zawsze przyrostowa - pełna dla każdego hosta ESX z węzłem narzędzia przenoszenia danych **dm1**.
- Harmonogram **bup_esxcluster_incr** codziennie uruchamia tworzenie kopii zapasowej typu zawsze przyrostowa - przyrostowa dla każdego hosta ESX z węzłem narzędzia przenoszenia danych **dm2**.

Wykonaj następujące czynności planowania kopii zapasowych w interfejsie GUI Data Protection for VMware vSphere:

- Uruchom interfejs GUI Data Protection for VMware vSphere, klikając ikonę w oknie Solutions and Applications (Rozwiązania i aplikacje) programu vSphere Client.
 - W oknie Pierwsze kroki kliknij kartę **Kopia zapasowa**, aby otworzyć okno Zarządzanie harmonogramami kopii zapasowych.
 - Znajdź harmonogram kopii zapasowej (używany dla kopii zapasowych typu zawsze przyrostowa - pełna lub przyrostowa) do zaktualizowania. W tej procedurze używany jest harmonogram typu zawsze przyrostowa - pełna (**bup_esxcluster_full**).
 - Prawym przyciskiem myszy kliknij ten harmonogram i wybierz opcję **Właściwości**.
 - Przejdź do strony Harmonogram i wybierz pozycję **Przyrostowa** z listy rozwijanej **Strategia kopii zapasowej**.
 - Kliknij przycisk **OK**, aby zapisać aktualizację.
 - Znajdź harmonogram kopii zapasowych używany dla kopii zapasowych typu zawsze przyrostowa - przyrostowa. Prawym przyciskiem myszy kliknij ten harmonogram i wybierz opcję **Usuń**. Ponieważ harmonogram typu zawsze przyrostowa - pełna (**bup_esxcluster_full**) został zaktualizowany do typu zawsze przyrostowa - przyrostowa, ten harmonogram typu zawsze przyrostowa - przyrostowa nie jest już potrzebny.
3. Teraz, gdy już istnieje harmonogram kopii zapasowych typu zawsze przyrostowa - przyrostowa, można zmniejszyć liczbę węzłów narzędzia przenoszenia danych przez ich konsolidację:

W tym przykładzie przedstawiono konsolidację dwóch węzłów narzędzia przenoszenia danych do jednego węzła narzędzia przenoszenia danych.

- Na serwerze kopii zapasowych vStorage otwórz wiersz komend i przejdź do katalogu, w którym znajduje się plik opcji węzła **dm1**.
- W edytorze tekstu (na przykład w notatniku) zaktualizuj ten plik, używając następujących opcji:
 - 1) Podaj **vmmaxparallel**, aby określić liczbę maszyn wirtualnych, których kopie zapasowe są jednocześnie tworzone przez węzeł **dm1**:
`vmmaxparallel=2`

Wartością domyślną i zarazem minimalną jest 1. Wartością maksymalną jest 50.

Wskazówka: Dla każdego usuwanego węzła narzędzia przenoszenia danych zwiększ wartość parametru `vmmaxparallel` o 1.

Alternatywnie można podać parametr `vmlimitperhost`, aby określić liczbę maszyn wirtualnych, których kopie zapasowe są jednocześnie tworzone przez węzeł `dm1` z tego samego hosta ESX:

```
vm limitperhost=1
```

Ta opcja jest przydatna do zabezpieczenia hosta przed przeciążeniem. Wartością domyślną jest 0 (brak limitu). Wartością minimalną jest 1. Wartością maksymalną jest 50.

- c. Zaloguj się do serwera IBM Spectrum Protect. Użyj administracyjnego klienta wiersza komend (`dsmdmc`), aby określić maksymalną liczbę jednoczesnych sesji tworzenia kopii zapasowych maszyn wirtualnych, które mogą być nawiązane z serwerem. Na przykład:
- ```
maxsessions=4
```

Wartością domyślną jest 25. Wartością minimalną jest 2.

4. Sprawdź, czy zaktualizowane węzły narzędzia przenoszenia danych działają poprawnie:
- Uruchom interfejs GUI Data Protection for VMware vSphere, klikając ikonę w oknie Solutions and Applications (Rozwiązania i aplikacje) programu vSphere Client.
  - W oknie Pierwsze kroki kliknij kartę Konfiguracja, aby wyświetlić stronę Status konfiguracji.
  - Na stronie Status konfiguracji wybierz serwer vCenter zabezpieczony w kroku 1. Kliknij węzeł narzędzia przenoszenia danych, aby wyświetlić jego status na panelu Szczegóły statusu. Gdy węzeł wyświetla ostrzeżenie lub komunikat o błędzie, kliknij ten węzeł i użyj informacji dostępnych na panelu Szczegóły statusu, aby rozwiązać problem. Następnie wybierz węzeł i kliknij opcję **Sprawdź poprawność wybranego węzła**, aby upewnić się, że problem został rozwiązany. Kliknij przycisk Odśwież, aby ponownie przetestować wszystkie węzły.

## Wyniki

Po pomyślnym zakończeniu każdej czynności środowisko jest gotowe do użycia w strategii kopii zapasowej typu zawsze przyrostowa - przyrostowa.

**Ograniczenia:** Po przeprowadzeniu migracji harmonogramów z typu kopii zapasowej zawsze przyrostowa - pełna do typów kopii zapasowej zawsze przyrostowa - przyrostowa należy pamiętać o następujących ograniczeniach:

- Zmiana zmigrowanych harmonogramów z powrotem do typów kopii zapasowej zawsze przyrostowa - pełna dla poszczególnych maszyn wirtualnych (obszar plików) nie jest obsługiwana.
- Użycie wcześniejszej wersji narzędzia przenoszenia danych programu IBM Spectrum Protect w zmigrowanym obszarze plików nie jest obsługiwane.
- Jeśli obszar plików zawiera jedną lub więcej kopii zapasowych typu zawsze przyrostowa - przyrostowa, kopia zapasowa typu zawsze przyrostowa - pełna nie jest obsługiwana.

## Przykład kontroli wersji za pomocą parametru `verexists`

W tym przykładzie migracji harmonogramu program Data Protection for VMware w wersji 6.3 używa dwóch harmonogramów tworzenia kopii zapasowych:

- `-mode=full`: zaplanowano tworzenie co tydzień kopii zapasowej typu zawsze przyrostowa - pełna (w niedziele), a maksymalna liczba wersji kopii zapasowych maszyn wirtualnych przechowywanych na serwerze wynosi cztery (`verexists=4`).

- `-mode=incr`: zaplanowano tworzenie w dni powszednie (od poniedziałku do soboty) kopii zapasowej typu zawsze przyrostowa - przyrostowa.

Liczba kopii zapasowych tworzonych w okresie czterech tygodni wynosi 28:

- Cztery kopie zapasowe typu zawsze przyrostowa - pełna (jedna tworzona co tydzień pełna kopia zapasowa pomnożona przez cztery tygodnie)
- 24 kopie zapasowe typu zawsze przyrostowa - przyrostowa (sześć przyrostowych kopii zapasowych tworzonych w dni powszednie pomnożonych przez cztery tygodnie)

Ponieważ w programie Data Protection for VMware w wersji 6.3 zliczane są tylko pełne kopie zapasowe, ustawienie `verexists=4` powoduje, że zachowywanych jest wszystkich 28 kopii zapasowych.

Aby zapewnić ten sam poziom ochrony za pomocą programu Data Protection for VMware w wersji 6.4 (lub nowszej) z zastosowaniem strategii kopii zapasowych typu zawsze przyrostowa - przyrostowa, należy utworzyć następujący harmonogram:

`-mode=iffull`: zaplanowano codzienne tworzenie kopii zapasowych typu zawsze przyrostowa - pełna, a dla parametru `verexists` ustawiono wartość 28.

Liczba kopii zapasowych tworzonych w okresie czterech tygodni wynosi 28:

- Jedna kopia zapasowa typu zawsze przyrostowa - pełna (początkowa kopia zapasowa pomnożona przez jeden dzień)
- 27 kopii zapasowych typu zawsze przyrostowa - przyrostowa (tworzona codziennie kopia zapasowa typu zawsze przyrostowa pomnożona przez 27 dni)

Ponieważ program Data Protection for VMware w wersji 6.4 (lub nowszej) zlicza zarówno kopie zapasowe typu zawsze przyrostowa - pełna, jak i typu zawsze przyrostowa - przyrostowa, ustawienie `verexists=28` powoduje zachowanie wszystkich 28 kopii zapasowych.



---

## **Dodatek C. Ułatwienia dostępu w rodzinie produktów IBM Spectrum Protect**

Ułatwienia dostępu umożliwiają niepełnosprawnym użytkownikom (np. niepełnosprawnym ruchowo lub niedowidzącym) korzystanie z technologii informatycznych.

### **Przegląd**

Rodzina produktów IBM Spectrum Protect obsługuje następujące główne funkcje ułatwień dostępu:

- obsługa wyłącznie za pomocą klawiatury;
- operacje z wykorzystaniem lektora ekranowego.

Rodzina produktów IBM Spectrum Protect używa najnowszego standardu W3C WAI-ARIA 1.0([www.w3.org/TR/wai-aria/](http://www.w3.org/TR/wai-aria/)) do zachowania zgodności z przepisami US Section 508([www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-section-508-standards/section-508-standards](http://www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-section-508-standards/section-508-standards)) i Web Content Accessibility Guidelines (WCAG) 2.0([www.w3.org/TR/WCAG20/](http://www.w3.org/TR/WCAG20/)). Aby skorzystać z ułatwień dostępu, należy użyć najnowszej wersji lektora ekranowego w połączeniu z najnowszą przeglądarką WWW obsługiwaną przez ten produkt.

Dokumentacja produktu w Centrum Wiedzy IBM obsługuje ułatwienia dostępu. Funkcje ułatwień dostępu w Centrum Wiedzy IBM zostały opisane w sekcji Ułatwienia dostępu w Centrum Wiedzy IBM([www.ibm.com/support/knowledgecenter/about/releasesnotes.html?view=kc#accessibility](http://www.ibm.com/support/knowledgecenter/about/releasesnotes.html?view=kc#accessibility)).

### **Nawigowanie przy użyciu klawiatury**

Ten produkt używa standardowych klawiszy nawigacyjnych.

### **Informacje na temat interfejsu**

Interfejs użytkownika produktu nie stosuje elementów, które migają z częstotliwością od 2 do 55 razy na sekundę.

Internetowy interfejs użytkownika wykorzystuje arkusze stylów CSS do wyświetlania treści. Aplikacja pozwala użytkownikom z wadą wzroku na używanie innych ustawień wyświetlania, w tym trybu wyświetlania o wysokim kontraście. Można regulować wielkość czcionki za pośrednictwem ustawień urządzenia lub przeglądarki WWW.

Interfejsy użytkownika zawierają elementy nawigacyjne WAI-ARIA, które umożliwiają szybkie przechodzenie między obszarami funkcjonalnymi aplikacji.

### **Oprogramowanie dostawcy**

Rodzina produktów IBM Spectrum Protect zawiera oprogramowanie pochodzące od innych dostawców, które nie jest objęte umową licencyjną firmy IBM. Firma IBM nie udziela żadnych gwarancji w zakresie ułatwień dostępu w tych produktach. Skontaktuj się z dostawcą, aby uzyskać informacje o ułatwieniach dostępu w tych produktach.

## Informacje pokrewne dotyczące ułatwień dostępu

Oprócz standardowych serwisów WWW działów pomocy telefonicznej i wsparcia firma IBM wprowadziła usługę telefonu tekstowego (TTY) dla niesłyszących lub niedosłyszących klientów pozwalającą uzyskać dostęp do usług handlowych i wsparcia:

Usługa TTY  
800-IBM-3383 (800-426-3383)  
(w Ameryce Północnej)

Więcej informacji na temat zaangażowania firmy IBM w upowszechnianie ułatwień dostępu można znaleźć w sekcji IBM Accessibility ([www.ibm.com/able](http://www.ibm.com/able)).

---

## Uwagi

Niniejsza publikacja została przygotowana z myślą o produktach i usługach oferowanych w Stanach Zjednoczonych. Niniejsza publikacja może być dostępna w innych wersjach językowych. Dostęp do niej może być jednak wymagać posiadania kopii produktu lub jego odpowiedniej wersji językowej.

IBM może nie oferować w innych krajach produktów, usług lub opcji omawianych w tej publikacji. Informacje na temat dostępnych produktów i usług można uzyskać od lokalnego przedstawiciela firmy IBM. Jakakolwiek wzmianka na temat produktu, programu lub usługi firmy IBM nie oznacza, że tylko ten produkt, program lub ta usługa mogą być używane. Dowolny, funkcjonalnie równoważny, produkt, program lub usługa, które nie naruszają jakichkolwiek praw własności intelektualnej firmy IBM, mogą być użyte. Jednakże cała odpowiedzialność za ocenę przydatności i sprawdzenie działania produktu, programu lub usługi, pochodzących od producenta innego niż IBM, spoczywa na użytkowniku.

Firma IBM może posiadać patenty lub złożone wnioski o patenty dotyczące informacji opisanych w tym dokumencie. Przedstawienie tej publikacji nie daje żadnych uprawnień licencyjnych do tychże patentów. Pisemne zapytania w sprawie licencji można przysyłać na adres:

*IBM Director of Licensing  
IBM Corporation  
North Castle Drive, MD-NC119  
Armonk, NY 10504-1785  
US*

Zapytania w sprawie licencji na informacje dotyczące zestawów znaków dwubajtowych (DBCS) należy kierować do lokalnych działów własności intelektualnej IBM (Intellectual Property Department) lub zgłaszać na piśmie pod adresem:

*Intellectual Property Licensing  
Legal and Intellectual Property Law  
IBM Japan Ltd.  
19-21, Nihonbashi-Hakozakicho, Chuo-ku  
Tokyo 103-8510, Japan*

INTERNATIONAL BUSINESS MACHINES CORPORATION DOSTARCZA TĘ PUBLIKACJĘ W STANIE, W JAKIM SIĘ ZNAJDUJE ("AS IS") BEZ UDZIELANIA JAKICHKOLWIEK GWARANCJI (W TYM TAKŻE RĘKOJMI), WYRAŻNYCH LUB DOMNIEMANYCH, A W SZCZEGÓLNOŚCI DOMNIEMANYCH GWARANCJI PRZYDATNOŚCI HANDLOWEJ, PRZYDATNOŚCI DO OKREŚLONEGO CELU ORAZ GWARANCJI, ŻE PUBLIKACJA NIE NARUSZA PRAW STRON TRZECICH.

Ustawodawstwa niektórych krajów nie dopuszczają zastrzeżeń dotyczących gwarancji wyraźnych lub domniemanych w odniesieniu do pewnych transakcji; w takiej sytuacji powyższe zdanie nie ma zastosowania.

Informacje zawarte w tej publikacji mogą zawierać nieścisłości techniczne lub błędy drukarskie. Informacje te są okresowo aktualizowane, a zmiany te zostaną ujęte w kolejnych wydaniach tej publikacji. IBM zastrzega sobie prawo do wprowadzania ulepszeń i/lub zmian w produktach i/lub programach opisanych w tej publikacji w dowolnym czasie, bez wcześniejszego powiadomienia.

Wszelkie wzmianki w tej publikacji na temat stron internetowych innych podmiotów zostały wprowadzone wyłącznie dla wygody użytkowników i w żadnym wypadku nie stanowią zachęty do ich odwiedzania. Materiały dostępne na tych stronach nie są częścią materiałów opracowanych dla tego produktu IBM, a użytkownik korzysta z nich na własną odpowiedzialność.

IBM ma prawo do używania i rozpowszechniania informacji przysyłanych przez użytkownika w dowolny sposób, jaki uzna za właściwy, bez żadnych zobowiązań wobec ich autora.

Licencjobiorcy tego programu, którzy chcieliby uzyskać informacje na temat programu w celu: (i) wdrożenia wymiany informacji między niezależnie utworzonymi programami i innymi programami (łącznie z tym opisywanym) oraz (ii) wspólnego wykorzystywania wymienianych informacji, powinni skontaktować się z:

*IBM Director of Licensing*  
*IBM Corporation*  
*North Castle Drive, MD-NC119*  
*Armonk, NY 10504-1785*  
*US*

Informacje takie mogą być udostępnione, o ile spełnione zostaną odpowiednie warunki, w tym, w niektórych przypadkach, zostanie uiszczona stosowna opłata.

Licencjonowany program opisany w niniejszej publikacji oraz wszystkie inne licencjonowane materiały dostępne dla tego programu są dostarczane przez IBM na warunkach określonych w Umowie IBM z Klientem, Międzynarodowej Umowie Licencyjnej IBM na Program lub w innych podobnych umowach zawartych między IBM i użytkownikami.

Omawiane tu dane o wydajności są przedstawione w postaci, w jakiej zostały otrzymane w określonych warunkach działania. Rzeczywiste wyniki mogą być inne.

Informacje dotyczące produktów firm innych niż IBM pochodzą od dostawców tych produktów, z opublikowanych przez nich zapowiedzi lub innych powszechnie dostępnych źródeł. Firma IBM nie testowała tych produktów i nie może potwierdzić skuteczności ich działania, kompatybilności lub jakichkolwiek innych danych związanych z produktami nie wytworzonymi przez firmę IBM. Pytania dotyczące produktów firm innych niż IBM należy kierować do dostawców tych produktów.

Publikacja ta zawiera przykładowe dane i raporty używane w codziennych operacjach działalności gospodarczej. W celu kompleksowego ich zilustrowania, podane przykłady zawierają nazwiska osób prywatnych, nazwy przedsiębiorstw oraz nazwy produktów. Wszystkie te nazwy/nazwiska są fikcyjne i jakiegokolwiek podobieństwo do istniejących nazw/nazwisk i adresów jest całkowicie przypadkowe.

#### LICENCJA W ZAKRESIE PRAW AUTORSKICH:

Niniejsza publikacja zawiera przykładowe aplikacje w kodzie źródłowym, ilustrujące techniki programowania na różnych platformach operacyjnych. Użytkownik może kopiować, modyfikować i dystrybuować te programy przykładowe w dowolnej formie bez uiszczania opłat na rzecz IBM w celu projektowania, używania, sprzedaży lub dystrybucji aplikacji zgodnych z aplikacyjnym interfejsem programowym dla tej platformy operacyjnej, dla której napisane zostały programy przykładowe. Programy przykładowe nie zostały gruntownie przetestowane. IBM nie może zatem gwarantować lub sugerować niezawodności, użyteczności i funkcjonalności tych programów. Programy przykładowe są dostarczane w stanie, w jakim się znajdują ("AS IS"), bez udzielania jakichkolwiek gwarancji. IBM nie ponosi odpowiedzialności za żadne szkody wynikłe z użycia programów przykładowych.



Każda kopia programu przykładowego lub jakiegokolwiek jego fragment, jak też jakiegokolwiek prace pochodne muszą zawierać następujące uwagi dotyczące praw autorskich: © (nazwa firmy) (rok). Fragmenty tego kodu pochodzą z programów przykładowych IBM Corp. © Copyright IBM Corp. \_wpisać rok lub lata\_.

## **Znaki towarowe**

IBM, logo IBM i ibm.com są znakami towarowymi International Business Machines Corp w Stanach Zjednoczonych i w innych krajach. Nazwy innych produktów i usług mogą być znakami towarowymi IBM lub innych firm. Aktualna lista znaków towarowych IBM jest dostępna na stronie WWW "Copyright and trademark information" pod adresem [www.ibm.com/legal/copytrade.shtml](http://www.ibm.com/legal/copytrade.shtml).

Adobe jest zastrzeżonym znakiem towarowym Adobe Systems Incorporated w Stanach Zjednoczonych i w innych krajach.

Linear Tape-Open, LTO i Ultrium są znakami towarowymi firm HP, IBM Corp. i Quantum w Stanach Zjednoczonych i w innych krajach.

Intel i Itanium są zastrzeżonymi znakami towarowymi lub znakami towarowymi Intel Corporation lub firm zależnych w Stanach Zjednoczonych i w innych krajach.

Linux.

Microsoft, Windows i Windows NT są znakami towarowymi firmy Microsoft Corporation w Stanach Zjednoczonych i w innych krajach.

Java oraz wszystkie znaki towarowe i logo dotyczące języka Java są znakami towarowymi lub zastrzeżonymi znakami towarowymi Oracle i/lub przedsiębiorstw afiliowanych Oracle.

UNIX jest zastrzeżonym znakiem towarowym The Open Group w Stanach Zjednoczonych i w innych krajach.

VMware, VMware vCenter Server i VMware są znakami towarowymi lub zastrzeżonymi znakami towarowymi firmy VMware, Inc. lub jej przedsiębiorstw podporządkowanych w Stanach Zjednoczonych i w innych krajach.

## **Warunki dotyczące dokumentacji produktu**

Zezwolenie na korzystanie z publikacji jest przyznawane na poniższych warunkach.

### **Przydatność**

Niniejsze warunki stanowią uzupełnienie warunków używania serwisu WWW IBM.

### **Użytek osobisty**

Użytkownik ma prawo kopiować te informacje do własnego, niekomercyjnego użytku, pod warunkiem zachowania wszelkich uwag dotyczących praw własności. Użytkownik nie ma prawa dystrybuować ani wyświetlać tych publikacji czy ich części, ani wykonywać z nich prac pochodnych bez wyraźnej zgody IBM.

### **Użytek służbowy**

Użytkownik ma prawo kopiować te publikacje, dystrybuować je i wyświetlać wyłącznie w ramach przedsiębiorstwa Użytkownika, pod warunkiem zachowania wszelkich uwag dotyczących praw własności. Użytkownik nie ma prawa wykonywać z tych publikacji ani z ich części prac pochodnych, kopiować ich ani wyświetlać poza przedsiębiorstwem Użytkownika bez wyraźnej zgody IBM.

## Uprawnienia

Z wyjątkiem zezwoleń wyraźnie udzielonych w niniejszym dokumencie, nie udziela się jakichkolwiek innych zezwoleń, licencji ani praw, wyraźnych czy domniemanych, odnoszących się do tych publikacji czy jakichkolwiek informacji, danych, oprogramowania lub innej własności intelektualnej, o których mowa w niniejszym dokumencie.

IBM zastrzega sobie prawo do anulowania zezwolenia przyznanego w niniejszym dokumencie w każdej sytuacji, gdy, według uznania IBM, korzystanie z tych publikacji jest szkodliwe dla IBM lub jeśli IBM uzna, że warunki niniejszego dokumentu nie są przestrzegane.

Użytkownik ma prawo pobierać, eksportować lub reeksportować niniejsze informacje pod warunkiem zachowania bezwzględnej i pełnej zgodności z obowiązującym prawem i przepisami, w tym ze wszelkimi prawami i przepisami eksportowymi Stanów Zjednoczonych.

IBM NIE UDZIELA ŻADNYCH GWARANCJI, W TYM TAKŻE RĘKOJMI, DOTYCZĄCYCH TREŚCI TYCH PUBLIKACJI. PUBLIKACJE TE SĄ DOSTARCZANE W STANIE, W JAKIM SIĘ ZNAJDUJĄ ("AS-IS") BEZ UDZIELANIA JAKICHKOLWIEK GWARANCJI, W TYM TAKŻE RĘKOJMI, WYRAŹNYCH CZY DOMNIEMANYCH, A W SZCZEGÓLNOŚCI DOMNIEMANYCH GWARANCJI PRZYDATNOŚCI HANDLOWEJ CZY PRZYDATNOŚCI DO OKREŚLONEGO CELU.

## Uwagi dotyczące strategii ochrony prywatności

Oprogramowanie IBM, w tym rozwiązanie SaaS (Software as a Service), zwane dalej "Oferowanym Oprogramowaniem", może korzystać z informacji cookie lub z innych technologii do gromadzenia danych o używaniu produktów, do poprawienia jakości usług dla użytkowników końcowych, do dopasowania interakcji do ich oczekiwań lub do innych celów. W wielu przypadkach Oferowane Oprogramowanie nie gromadzi informacji pozwalających na identyfikację osoby. Część Oferowanego Oprogramowania może jednak umożliwiać gromadzenie informacji pozwalających na identyfikację osoby. Jeśli Oferowane Oprogramowanie korzysta z informacji cookie do gromadzenia informacji pozwalających na identyfikację osoby, poniżej znajdują się szczegółowe informacje na temat takiego korzystania.

To oprogramowanie nie używa informacji cookie ani innych technologii do gromadzenia informacji pozwalających na identyfikację osoby.

Jeśli konfiguracje Oferowanego Oprogramowania umożliwiają gromadzenie informacji pozwalających na identyfikację użytkowników końcowych za pośrednictwem informacji cookie lub innych technologii, należy wystąpić o poradę prawną w zakresie prawa obowiązującego przy takim gromadzeniu danych, w tym wymagań dotyczących powiadomienia i zgody.

Więcej informacji na temat korzystania z różnych technologii, w tym z informacji cookie, do opisanych wyżej celów znajduje się w serwisie IBM's Privacy Policy pod adresem <http://www.ibm.com/privacy> i w publikacji IBM Online Privacy Statement pod adresem <http://www.ibm.com/privacy/details> w sekcji zatytułowanej "Cookies, Web Beacons and Other Technologies" i w publikacji "IBM Software Products and Software-as-a-Service Privacy Statement" pod adresem <http://www.ibm.com/software/info/product-privacy>.

---

## **Glosariusz**

Udostępniono glosariusz z terminami i definicjami dla rodziny produktów IBM Spectrum Protect.

Patrz Glosariusz dla produktu IBM Spectrum Protect.



---

# Indeks

## A

- agent odtwarzania 6
- akceptor klienta
  - konfigurowanie 113
- aktualizacja cicha
  - Linux 33
  - Windows, wersja 64-bitowa 32
- aktualizowanie
  - Linux
    - tryb cichy 33
  - przegląd 31
  - Windows, wersja 64-bitowa
    - tryb cichy 32
  - z wersji 6.x
    - standardowe 31

## C

- Centrum Wiedzy v
- certyfikat innej firmy
  - dostęp do magazynu kluczy 65
  - konfigurowanie protokołu TLS 64
  - odbieranie podpisanego certyfikatu 67
  - tworzenie żądania podpisania certyfikatu 66
  - wysłanie żądania podpisania certyfikatu 67

## D

- Data Protection for VMware
  - komponenty instalowalne 1
  - planowanie 10
  - pobieranie pakietu 22
- deinstalacja cicha
  - Linux
    - tryb cichy 36
  - Windows, wersja 64-bitowa
    - tryb cichy 35
- deinstalowanie
  - Linux
    - tryb cichy 36
    - typowe 34
  - Windows, wersja 64-bitowa
    - tryb cichy 35
    - typowe 34
- dostęp do magazynu kluczy
  - certyfikat innej firmy 65

## G

- GUI
  - interfejs GUI Data Protection for VMware vSphere 30

## I

- IBM, Centrum Wiedzy v
- informacje autoryzacyjne
  - uprawnienia 16
- instalacja cicha
  - Linux 28

- instalacja cicha (*kontynuacja*)
  - Windows, wersja 64-bitowa
    - tryb cichy, Suite Installer 27
- instalowanie
  - Data Protection for VMware 1
  - komponenty 22
  - komponenty instalowalne 1
  - Linux
    - za pomocą kreatora instalacji 25
  - pobieranie pakietu 22
  - przewodnik przejścia 10
  - uprawnienia użytkownika 16
  - uzyskiwanie pakietu 22
  - Windows
    - za pomocą kreatora instalacji 23
  - wymagane porty komunikacyjne 16
  - wymagania programowe 12
  - wymagania sprzętowe 12
  - wymagania systemowe 12
- interfejs GUI Data Protection for VMware vSphere 3, 30
  - uprawnienia
    - operacje 72
- interfejs GUI odtwarzania plików 8
- interfejs GUI programu agent odtwarzania
  - konfigurowanie 76
  - opcje 76
- interfejs GUI vSphere 30
- interfejs wiersza komend Data Protection for VMware 7

## K

- klawiatura 123
- klucz rejestracji 75
- komponenty 1
  - agent odtwarzania 6
  - interfejs GUI Data Protection for VMware vSphere 3
  - interfejs GUI odtwarzania plików 8
  - interfejs wiersza komend Data Protection for VMware 7
  - komponenty instalowalne 22
  - narzędzie przenoszenia danych 8
  - wtyczka klienta IBM Spectrum Protect vSphere 6
- komponenty instalowalne 1
  - interfejs GUI Data Protection for VMware vSphere 3
  - interfejs GUI odtwarzania plików 8
  - interfejs wiersza komend Data Protection for VMware 7
  - narzędzie przenoszenia danych 8
  - wtyczka klienta IBM Spectrum Protect vSphere 6
- komunikacja TLS
  - konfigurowanie 62
- konfigurowanie
  - akceptor klienta 113
  - arkusz dla programu Data Protection for VMware 29
  - czynności zaawansowane 89
  - interfejs GUI programu agent odtwarzania 76
  - istniejąca konfiguracja 42
  - komunikacja przeglądarki WWW 62
  - komunikacja TLS 62
  - konfiguracja początkowa 41
  - odtworzenie plików
    - opcje 45
  - plik konfiguracyjny interfejsu VMCLI 115

- konfigurowanie *(kontynuacja)*
  - podłączanie iSCSI 104, 107
  - przegląd 41
  - SSL 62
  - środowisko vSphere
    - lista kontrolna wiersza komend 99
  - taśmowa pamięć masowa 102
  - ustawienia narodowe 84
  - VMCLI
    - środowisko vSphere 97
  - węzły IBM Spectrum Protect
    - środowisko vSphere 90
  - węzły narzędzia przenoszenia danych
    - środowisko vSphere 91, 93
  - węzły proxy podłączania
    - Linux 109
    - Windows 111
  - włączanie obsługi znaczników 48
  - włączenie odtwarzania plików 43
- konfigurowanie protokołu TLS
  - certyfikat innej firmy 64
  - ośrodek certyfikacji 64
  - włączanie bezpiecznej komunikacji z serwerem 63, 81, 83
- kreатор instalacji
  - Linux
    - za pomocą kreatora instalacji 25
  - Windows
    - za pomocą kreatora instalacji 23
- kreатор konfiguracji 41

## L

- Linux
  - aktualizowanie
    - tryb cichy 33
  - deinstalowanie
    - tryb cichy 36
    - typowe 34
  - procedura instalacji
    - czysta 25
    - tryb cichy 28

## M

- migrowanie
  - harmonogramy 117
- modyfikowanie
  - przegląd 38
- modyfikowanie instalacji 39

## N

- narzędzie przenoszenia danych 8
  - węzły
    - konfigurowanie w środowisku vSphere 91, 93
- niepełnosprawność 123
- notatnik konfiguracji 42
- nowości w programie Data Protection for VMware w wersji 8.1.6 vii

## O

- obsługa znaczników
  - włączenie 48
- odbieranie podpisanego certyfikatu
  - certyfikat innej firmy 67

- odtworzenie
  - agent odtwarzania 6
  - konfigurowanie opcji 45
  - konfigurowanie rejestrowania 47
  - opcje 46, 48
  - plik 14, 45, 46, 47, 48
  - wymagania wstępne 14
- odtworzenie plików
  - konfigurowanie opcji 45
  - konfigurowanie rejestrowania 47
  - opcje 46, 48
  - środowisko systemu Linux 44
  - włączenie 43
  - wymagania wstępne 14
- opcje przetwarzania
  - używanie 56, 57, 60

## P

- planowanie
  - przegląd 10
  - przewodnik przejścia 10
  - uprawnienia 16
  - wymagane porty komunikacyjne 16
  - wymagania systemowe 12
- plik konfiguracyjny interfejsu VMCLI
  - modyfikowanie 115
  - vmcliConfiguration.xml 115
- podłączanie iSCSI
  - konfigurowanie 104, 107
- porty
  - instalowanie 16
- porty komunikacyjne
  - instalowanie 16
- procedura instalacji
  - Linux
    - czysta 25
    - tryb cichy 28
  - Windows, wersja 64-bitowa
    - tryb cichy, Suite Installer 27
- publikacje v

## R

- rejestrowanie
  - odtworzenie plików 47

## S

- SSL
  - konfigurowanie 62, 63, 81, 83

## T

- taśmowa pamięć masowa
  - konfigurowanie 102
- tworzenie żądania podpisania certyfikatu
  - certyfikat innej firmy 66

## U

- ułatwienia dostępu 123
- uprawnienia
  - instalowanie 16

- uprawnienia (*kontynuacja*)
  - interfejs GUI Data Protection for VMware vSphere
    - operacje 72
- uprawnienia administratora
  - interfejs GUI Data Protection for VMware vSphere 72
- uprawnienie
  - uprawnienia 16
- usługi 87
- ustawienia narodowe
  - ustawienia 84
- użytkownik
  - uprawnienia 16

## V

- VMCLI
  - konfigurowanie w środowisku vSphere 97

## W

- węzły IBM Spectrum Protect
  - konfigurowanie
    - środowisko vSphere 90
- Windows, wersja 64-bitowa
  - aktualizowanie
    - tryb cichy 32
  - deinstalowanie
    - tryb cichy 35
  - typowe 34
  - procedura instalacji
    - tryb cichy, Suite Installer 27
- włączanie bezpiecznej komunikacji z serwerem
  - konfigurowanie protokołu TLS 63, 81, 83
- wtyczka klienta IBM Spectrum Protect vSphere 6
- wymagania programowe 12
- wymagania sprzętowe 12
- wymagania systemowe 12
- wysłanie żądania podpisania certyfikatu
  - certyfikat innej firmy 67









Numer Programu: 5725-X00

Drukowane w USA