

Często zadawane pytania: Dell PowerProtect Data Manager

Spis treści

Często zadawane pytania: Dell PowerProtect Data Manager	1
Przegląd	2
Nowości w programie PowerProtect Data Manager w wersji 19.19 (marzec 2025 r.)	3
Nowości w programie PowerProtect Data Manager w wersji 19.18 (listopad 2024 r.).....	3
Nowości w programie PowerProtect Data Manager w wersji 19.17 (lipiec 2024 r.)	4
Nowości w programie PowerProtect Data Manager w wersji 19.16 (marzec 2024 r.)	5
Nowości w programie PowerProtect Data Manager w wersji 19.15 (listopad 2023 r.).....	6
Nowości w programie PowerProtect Data Manager w wersji 19.14 (lipiec 2023 r.)	7
Nowości w programie PowerProtect Data Manager w wersji 19.13 (marzec 2023 r.)	8
Nowości w programie PowerProtect Data Manager w wersji 19.12 (październik 2022 r.)	9
Nowości w programie PowerProtect Data Manager w wersji 19.11 (czerwiec 2022 r.).....	10
Nowości w programie PowerProtect Data Manager w wersji 19.10 (marzec 2022 r.)	11
Nowości w programie PowerProtect Data Manager w wersji 19.9 (wrzesień 2021 r.).....	13
Wprowadzenie wersji PowerProtect Data Manager Essentials (czerwiec 2021 r.)	14
Nowości w programie PowerProtect Data Manager w wersji 19.8 (maj 2021 r.).....	14
Nowości w programie PowerProtect Data Manager w wersji 19.7 (luty 2021 r.)	16
Nowości w programie PowerProtect Data Manager w wersji 19.6 (październik 2020 r.)	17
Nowości w programie PowerProtect Data Manager w wersji 19.5.....	18
Czym jest oprogramowanie PowerProtect Data Manager?.....	18
Funkcje oprogramowania PowerProtect Data Manager	21
PowerProtect Data Manager	22
Optymalizacja pod kątem wielu chmur	25
Application Direct	26
Agent systemu plików	27
Wtyczka systemu plików DDBoost (BoostFS)	27
Obsługa produktów VMware i wirtualizacji.....	28
Obsługa monitora maszyn wirtualnych Hyper-V	32

Storage Direct Protection	33
Storage Direct Protection z Dell Storage	34
Wykrywanie anomalii	36
Archiwizacja do obiektu	38
Raportowanie wielu systemów	39
Oparta na chmurze analityka i monitorowanie	40
Ochrona obciążeń roboczych w chmurze oparta na modelu SaaS	41
PowerProtect Cyber Recovery	42
Path to PowerProtect	43
Nowoczesna architektura oparta na usługach	45
Zasoby z zakresu wspierania sprzedaży	45
Licencjonowanie	45
Zamawianie i pomoc techniczna	45

Przegląd

Data protection software offer components

Capability / Name	PowerProtect Data Manager + (Plus)	Data Protection Suite	Data Protection Suite + (Plus)	PowerProtect Data Manager Essentials
PowerProtect Data Manager	Y	Y	Y	Y
App Direct (MS App, DB App, Oracle RMAN & FS Agents)	Y	Y	Y	Y
Storage Direct (Storage Direct Agent)	Y	Y	Y	Y
PowerProtect Cloud Snapshot Manager	Y	Y	Y	Y
Cloud Disaster Recovery	Y	Y	Y	Y
RecoverPoint for Virtual Machines	Y	Y	Y	Y
PowerProtect Cyber Recovery	Y	Y	Y	Y
vRealize Data Protection Extension	Y	Y	Y	Y
DD Boost FS	Y	Y	Y	Y
Microsoft Granular Recovery (GLR / ItemPoint)	Y	Y	Y	Y
Data Protection Central	Y	Y	Y	Y
vProtect	Y	Y	Y	Y
NetWorker (including CloudBoost and vRealize DP Extension) and NetWorker Virtual Edition		Y	Y	
Avamar (including vRealize DP Extension) & Avamar Virtual Edition		Y	Y	
Data Protection Advisor	Y	Y	Y	Y
Search	Embedded	Embedded	Y	Embedded
Cloud Tier	Y		Y	Y
APEX Protection Storage	Y		Y	Y

Nowości w programie PowerProtect Data Manager w wersji 19.19 (marzec 2025 r.)

Ulepszenia dotyczące obciążeń roboczych

- Rozszerzona obsługa ekosystemu: monitor maszyn wirtualnych Hyper-V, Azure Local, OpenShift Virtualization, PostgreSQL
- Migawki Transparent Snapshot: Obsługa silnika wirtualnych maszyn Google Cloud Vmware Engine (GCVE)
- Przywracanie systemu plików do folderu Nowe/Alternatywne, system plików indeksu XFS dla kopii zapasowych BBB
- NAS: obsługa listy plików zmian PowerScale/Isilon, obsługa funkcji NetApp Multi-Node HA

Ulepszone zabezpieczenia

- Wykrywanie anomalii (GA)
- Uwierzytelnianie wieloskładnikowe (MFA): Google Authenticator i Microsoft Authenticator

Ulepszenia dotyczące wygody użytkowników

- Raportowanie wielu systemów
- Archiwizacja do obiektu dla maszyn wirtualnych i systemów plików — tylko ECS
- Data Manager, ochrona VMware-HA
- Obsługa opcji ręcznej aktualizacji serwera proxy dla klientów
- Obsługa zlokalizowanych systemów operacyjnych — j. portugalski (Brazylia)

Storage Direct Protection

- Obsługa szybkiego odzyskiwania
- Narzędzie CLI do tworzenia kopii zapasowych i przywracania danych
- PowerMax
 - Automatyczne tworzenie grupy pamięci masowej przywracania
 - Przywróć mapowanie woluminu/grupy pamięci masowej

Więcej informacji można znaleźć w [prezentacji dotyczącej nowości w oprogramowaniu PowerProtect Data Manager 19.19](#).

Nowości w programie PowerProtect Data Manager w wersji 19.18 (listopad 2024 r.)

Dell Storage

- PowerMax
 - Lokalne zarządzanie migawkami za pomocą Storage Direct Protection
 - [MEDITECH](#), odtwarzanie serwera po awarii

- Ulepszenia wydajności (operacje na mapach bitowych migawek, przywracanie używanych bloków)
- Autonomiczne narzędzie do przywracania awaryjnego
- PowerMax i PowerStore
 - Włączanie/wyłączanie szyfrowania DDBoost
 - Licencjonowana kolekcja rozmiarów
 - Obsługa ponownego uruchamiania zadań ochrony

Ulepszone zabezpieczenia

- Wykrywanie anomalii (wersja Tech Preview)
- Konfigurowalne wygasanie certyfikatu głównego

Ulepszenia dotyczące obciążeń roboczych

- NAS — obsługa wielu sieci VLAN, integracja migawek w jednym węźle za pomocą NetApp
- Wyświetlanie kopii Avamar w interfejsie użytkownika programu PowerProtect Data Manager
- Opcja automatycznej instalacji Transparent Snapshots VIB
- Ulepszona równoległa kopia zapasowa PowerProtect Data Domain HA z TSDM

Uaktualnienia baz danych

- Równoległość na poziomie hosta SQL po stronie klienta dla kopii zapasowych
- Szczegółowe przywracanie usługi Active Directory przy użyciu członkostwa w grupach użytkowników

Ulepszenia dotyczące wygody użytkowników

- Kopie: funkcja wyszukiwania tagów w architekturze Data Invulnerability Architecture (DIA)
- Obsługa zlokalizowanych systemów operacyjnych — j. portugalski (Brazylia)
- Obsługa systemów PowerMax 10.2.0, DDOS 8.1, AlmaLinux

Więcej informacji można znaleźć w [prezentacji dotyczącej nowości w oprogramowaniu PowerProtect Data Manager 19.18](#).

Nowości w programie PowerProtect Data Manager w wersji 19.17 (lipiec 2024 r.)

Obsługa obciążeń roboczych

- Integracja rozwiązania PowerMax Storage Direct Protection
- PowerStore Storage Direct Protection z kopiami zapasowymi spójnymi z aplikacjami
- Obsługa Oracle Exadata i agent systemu Windows dla Oracle RMAN
- Wybór kompresji zoptymalizowany pod kątem aplikacji

- Wielostrumieniowe kopie zapasowe plików i bloków dla systemu Linux
- Szybkie przywracanie AppAware SQL do alternatywnego wsparcia technicznego
- Obsługa File System Agent dla systemu operacyjnego Debian Linux 9 i 10

Ulepszone zabezpieczenia

- Wykrywanie anomalii (beta)
- Monit/logowanie VMware 2FA z odzyskiwaniem na poziomie plików
- Generowanie dzienników kontrolnych dla nadchodzących wygaśnień certyfikatów innych firm
- Obsługa pośredniego podpisywania CA
- Alerty dotyczące brakujących dzienników

Udoskonalenia NAS

- Obsługa tworzenia kopii zapasowych udziałów i plików NAS z uprawnieniami 700, 500, 400
- Włączanie przekierowania przywracania plików NAS w ramach tego samego udziału
- Opcja unikania nadpisywania podczas operacji przywracania NAS
- Obsługa szybkiego odzyskiwania

Ulepszenia dotyczące wygody użytkowników

- Ulepszone śledzenie wykorzystania FETB dla zasobów i zasad ochrony (maszyny wirtualne, agenty, K8)
- RBAC dla skryptu przed/po
- Zarządzanie poprawkami za pomocą interfejsów użytkownika
- Zlokalizowana obsługa systemów operacyjnych – chiński tradycyjny i hiszpański

Więcej informacji można znaleźć w [prezentacji dotyczącej nowości w oprogramowaniu PowerProtect Data Manager 19.17](#).

Nowości w programie PowerProtect Data Manager w wersji 19.16 (marzec 2024 r.)

Ulepszenia dotyczące wygody użytkowników

- Filtry plików: dodanie opcji dołączania, dodatkowe filtry i zaprojektowany od nowa interfejs użytkownika dla kopii zapasowych opartych na plikach i NAS
- Skrypty wstępne i końcowe dotyczące zasad ochrony agenta aplikacji
- Zarządzanie katalogami kopii, w tym wyszukiwanie, usuwanie i przechowywanie aktualizacji między kopiami
- Kreator z instrukcjami dotyczącymi działań związanych z ochroną

- Samoobsługowe kopie zapasowe niewymagające uprawnień administratora dla SQL, Oracle RMAN, systemu plików i SAP HANA na platformie Unix.
- Ulepszenia dotyczące generowania dzienników
- System DDOS 8.0 działający na sprzęcie szesnastej generacji
- Obsługa rozwiązania vSphere 8.0 U2
- Obsługa migawek Transparent Snapshot i VADP dla VMS w ramach rozwiązania vSAN ESA
- Szybszy odczyt małych plików w systemie plików FNSv3
- Obsługa systemu NAS FS w wersji 4.1/4.2

Obsługa obciążeń roboczych

- Lista certyfikowanych dostawców SAP dla SAP HANA
- Szybkie odzyskiwanie w środowiskach SQL App Direct, SAP HANA, Exchange, Oracle i VMware FLR
- Przywracanie usuniętych maszyn wirtualnych z oryginalnymi identyfikatorami UUID
- Obsługa Oracle Exadata (wersja Tech Preview)
- Oracle — zwiększona wydajność tworzenia kopii zapasowych dla kompresji i bazy danych z obsługą TDE
- Exchange — odzyskiwanie wielu baz danych
- Obsługa przywracania danych Distributed Resources Scheduler (DRS)
- Restartowanie uruchomionych zadań po uaktualnieniu
- Indeksowanie systemów plików ZFS

Więcej informacji można znaleźć w [prezentacji dotyczącej nowości w oprogramowaniu PowerProtect Data Manager 19.16](#).

Nowości w programie PowerProtect Data Manager w wersji 19.15 (listopad 2023 r.)

Ulepszona obsługa obciążeń roboczych

- Scentralizowane przywracanie w środowisku SAP HANA
- Scentralizowane przywracanie w środowisku Exchange
- Oracle RAC — kopie zapasowe z wielu strumieni i tryb aktywny/pasywny
- Autonomiczny agent Hadoop
- Baza danych MetaCache (MCDB) w środowisku Exchange 2019
- Optymalizacja fragmentatora dla systemów plików NAS o dużej gęstości z dynamiczną ochroną NAS
- Tworzenie kopii zapasowych do bezpośredniej ochrony magazynów blokowych bezpośrednio w pamięci masowej do ochrony danych APEX

Ulepszenia dotyczące systemów plików

- Szczegółowe odzyskiwanie danych usługi Active Directory

- Współistnienie agenta systemu plików (FSA) z agentami DDBEA i Data Manager
- Możliwość wyboru kopii zapasowej opartej na blokach lub na plikach
- Obsługa systemu Rocky Linux w wersjach 8 i 9
- Obsługa woluminów ZFS

Ulepszone zabezpieczenia

- Szyfrowanie metadanych i dzienników systemowych
- Funkcja zarządzania replikacją plików (MFR) automatycznie wybiera najbezpieczniejszą dostępną opcję
- Ścisła weryfikacja publicznego interfejsu API REST
- Opcja usunięcia funkcji zarządzania blokadą retencji (RLG) z wybranej kopii zapasowej
- Integracja zgodności blokady replikacji (RLC) i mechanizmu raportowania dla rozwiązania PowerStore

Lepsze wrażenia klientów

- Obsługa nazw zasobów i źródeł zasobów w języku koreańskim
- Klonowanie zasad ochrony
- Automatyczne wznawianie zadań dla agentów NAS i aplikacji po uaktualnieniu
- Wykrywanie kopii utworzonych po zdarzeniu odzyskiwania po awarii
- Wyświetlanie źródła pochodzenia zadań (zaplanowane, ręczne)
- Różnice ochrony między najnowszymi a poprzednimi zadaniami (liczba zasobów, rozmiar kopii zapasowej, czas trwania)

Więcej informacji można znaleźć w [prezentacji dotyczącej nowości w oprogramowaniu PowerProtect Data Manager 19.15](#).

Nowości w programie PowerProtect Data Manager w wersji 19.14 (lipiec 2023 r.)

Obsługa urządzeń

- Obsługa macierzy pamięci masowej PowerStore
 - Tworzenie przyrostowych kopii zapasowych bez ograniczeń i odzyskiwanie danych z woluminów PowerStore do PowerProtect Data Domain/APEX Protection Storage i DM5500
 - Zarządzanie lokalnymi migawkami PowerStore za pomocą programu Data Manager
 - Spójne z awariami tworzenie kopii zapasowych i odzyskiwanie danych ze scentralizowanym zarządzaniem
 - Obsługa natychmiastowego dostępu z kopii DD
 - Przywracanie danych do pierwotnych i alternatywnych macierzy PowerStore z kopii podstawowej / repliki

- Kwalifikacja Oracle Database Appliance (ODA)

Ulepszenia dotyczące rozwiązań VMware i kontenerów

- Aranżacja odzyskiwania
 - Szybkie, elastyczne i szczegółowe przywracanie danych maszyn wirtualnych
- Obsługa ochrony uwzględniającej specyfikę aplikacji dla SQL za pomocą migawek Transparent Snapshot
- Ulepszone widoki zasobów dla maszyn wirtualnych w oknie Zasoby i zasady
- Równoległa ochrona klastrów Kubernetes

Ulepszone zabezpieczenia

- Odświeżenie certyfikatów innych firm
- Ulepszona wydajność szyfrowania podczas przesyłania danych

Nowe funkcje związane z chmurą

- Obsługa rozwiązania Oracle Cloud VMware Solution (OCVS)
- Obsługa odzyskiwania po awarii w chmurze dla platformy AWS w regionie APJ-Southeast-3

Szczegółowa kontrola

- Konfigurowalne porty dla agentów aplikacji
- Konfigurowalne limity ograniczania przepustowości dla hostów agenta aplikacji
- Obsługa zmian adresu IP DHCP agenta

Lepsze wrażenia klientów

- Konfiguracja strefy czasowej interfejsu użytkownika
- Zaplanowane raporty e-mail
- Stan indeksowania w wyszukiwarkach
- Kroki zadań konfiguracji dla agentów aplikacji
- Ulepszenia dotyczące wstępnego sprawdzania przepływu pracy aktualizacji systemu
- Ulepszone procesy ponownego przypisywania adresów IP i wymiany pamięci masowej

Więcej informacji można znaleźć w [prezentacji dotyczącej nowości w oprogramowaniu PowerProtect Data Manager 19.14](#).

Nowości w programie PowerProtect Data Manager w wersji 19.13 (marzec 2023 r.)

Ulepszenia dotyczące obciążeń roboczych

- Oracle Incremental Merge (OIM)
 - Tworzenie kopii zapasowej Oracle na poziomie obrazu

- Natychmiastowy dostęp i funkcje montowania obrazów na żywo
 - Obsługa sfederowanych kopii zapasowych Oracle Data Guard
 - Dynamiczna pamięć masowa NAS
 - Obsługa protokołu IPv6
 - Obsługa wielu sieci VLAN zapewniająca większą elastyczność
 - Odświeżanie agenta autonomicznego
 - Równoczesne korzystanie z agenta Data Manager i agenta autonomicznego
 - Zlokalizowana obsługa zasobów (i źródeł zasobów) w systemie operacyjnym
 - Optymalizacja pamięci systemu
 - Cloud Snapshot Manager
 - Obsługa platformy Google Cloud
 - Integracja z magazynem Cyber Recovery na platformie Azure (beta)
 - Szyfrowanie w locie na potrzeby ochrony maszyn wirtualnych
- Ulepszone zabezpieczenia
- Uwierzytelnianie dwuskładnikowe RSA SecurID
 - Szyfrowanie w locie na potrzeby ochrony maszyn wirtualnych
- Ulepszone funkcje dotyczące chmury
- Cloud Snapshot Manager
 - Obsługa platformy Google Cloud
 - Integracja z magazynem Cyber Recovery na platformie Azure (beta)

Nowości w programie PowerProtect Data Manager w wersji 19.12 (październik 2022 r.)

Zmiany dotyczące obciążeń roboczych

- Ulepszenia w zakresie dynamicznej pamięci masowej NAS
 - Ulepszone funkcje rozwiązywania PowerScale umożliwiające bezproblemowe wprowadzanie urządzeń PowerScale skonfigurowanych z wieloma strefami dostępu i strefami SmartConnect
 - Możliwość pobierania dzienników pominiętych elementów, wyświetlania pominiętych elementów, których kopia zapasowa nie została utworzona w ramach ochrony udziału NAS z powodu problemów z listą ACL lub plikami, a także filtrowania pominiętych elementów w zależności od kategorii problemu

- Ulepszenia dotyczące maszyn wirtualnych
 - Zwiększono z 10 do 20 liczbę jednoczesnych operacji tworzenia kopii zapasowych i przywracania maszyn wirtualnych TSDM, co pozwala zwiększyć przepustowość i skrócić czas tworzenia kopii zapasowych
 - Pakiet instalacyjny vSphere (VIB) został zoptymalizowany, aby wykrywał, czy oprogramowanie już istnieje w magazynie danych, i przysyłał VIB tylko wtedy, gdy oprogramowanie nie jest współdzielone przez hosty ESXi.
- Obsługa funkcji Oracle Data Guard (tylko wersja autonomiczna)
- Ulepszenia dotyczące platformy Kubernetes
 - Możliwość aktualizacji pól konfiguracji kontrolera PowerProtect, Velero lub cProxy, które można wykorzystać w celu dodania kart interfejsu sieciowego (NIC) lub ustawienia konfiguracji DNS dla zasobników.

Większe bezpieczeństwo

- Protokół IPv6 jest obsługiwany przez rdzeń programu PowerProtect Data Manager, agenty aplikacji i kopie zapasowe maszyn wirtualnych.
- Możliwość skonfigurowania jednostek pamięci masowej i zasad ochrony, aby włączyć blokadę przechowywania w trybie zgodności w pamięci masowej ochrony.

Łatwa obsługa

- Wprowadzenie okna Zadania dotyczące zasobów.
- Możliwość identyfikowania konfliktów harmonogramów w ramach zasad ochrony i odpowiedniego dostosowywania harmonogramów.
- Raporty e-mail

Nowości w programie PowerProtect Data Manager w wersji 19.11 (czerwiec 2022 r.)

Ulepszona obsługa

- Integracja z pamięcią masową Dell ISG
 - Obsługa tworzenia migawek PVC Kubernetes dla tej samej grupy woluminów
 - Korzystanie z rozszerzenia migawek grupy woluminów sterownika CSI PowerFlex
- Obsługa ochrony migawek PVC przydzielanych w różnych strefach dostępu PowerScale
 - Służy do zezwalania na dostęp lub odmawiania dostępu do woluminów znajdujących się w tych strefach

- Obsługa scentralizowanej ochrony danych Oracle
- Obsługa agenta Oracle RMAN z oprogramowaniem Oracle 21c
- Możliwość wysyłania aktualizacji do wszystkich agentów z centralnego serwera PowerProtect Data Manager
- Obsługa szyfrowania danych kopii zapasowych i przywracania danych podczas przesyłania zasobów klastra Kubernetes

Większe bezpieczeństwo

- Kontrola dostępu na poziomie wystąpienia RBAC
 - Możliwość szczegółowej kontroli zasobów
 - Klienci mogą ograniczyć uprawnienia tylko do tego, co jest wymagane do ochrony danych
 - Ochrona administracyjna nie jest wymagana
- Umożliwienie kontom systemowym bez uprawnień administratora odnajdowania, tworzenia kopii zapasowych i przywracania zasobów SQL

Ulepszone funkcje

- Replikacja podstawowej kopii zapasowej po ukończeniu
- Obsługa przekazywania serwera syslog
- Możliwość eksportowania tabel z interfejsu użytkownika PowerProtect Data Manager do plików CSV
- Ulepszenia dotyczące raportowania lokalnego

Nowości w programie *PowerProtect Data Manager* w wersji 19.10 (marzec 2022 r.)

Ulepszona obsługa

- Podgląd techniczny funkcji raportowania lokalnego
 - Zaktualizowane pulpity nawigacyjne: widżety Zadania, Zasoby, Kondycja, Zgodność, Pojemność i Optymalizacja przestrzeni
 - Szczegółowe raporty dotyczące wskaźników KPI
 - Podsumowanie ochrony zasobów
 - Zadania tworzenia kopii zapasowych, przywracania i replikacji
 - Możliwość monitorowania zadań samoobsługowych z poziomu konsoli PowerProtect Data Manager

Ulepszenia funkcji i przypadków użycia

- Ulepszenia dotyczące systemów plików
 - Odzyskiwanie systemu od podstaw w celu umożliwienia przywrócenia całego systemu operacyjnego Windows i danych
 - Obsługa nowych platform: Windows Server 2022 i AIX
 - Rozpoznawanie klastrów Windows FS
 - Dodano opcję widoku interfejsu użytkownika umożliwiającą przełączanie się między widokiem listy wszystkich zasobów systemu plików a hierarchicznym widokiem zasobów w obrębie każdego hosta systemu plików, który został wykryty w programie Data Manager
- W chmurze
 - Możliwość przenoszenia lokalnych migawek VMware Transparent Snapshot do chmur Azure lub AWS w celu ułatwienia odtwarzania po awarii (DR) w chmurze
 - Kopie zapasowe przechowywane w puli systemu DD Smart Scale obsługują funkcję Cloud DR
- VMware
 - Zwiększona wydajność rozwiązania Transparent Snapshots Data Manager (TSDM)
 - Rozwiązanie TSDM zostało zoptymalizowane pod kątem zwiększenia przepustowości przywracania i efektywniejszego spełnienia wymagań dotyczących czasu odzyskiwania maszyn wirtualnych
 - Zasady maszyn wirtualnych skonfigurowane w trybie optymalizacji pojemności będą teraz mogły korzystać z ochrony opartej na TSDM
 - Obsługa woluminów VVOL
 - Włączono funkcję CDR dla migawek Transparent Snapshot
 - Przywracanie maszyn wirtualnych
 - Pomijanie Kontroli konta użytkownika w przypadku przywracania danych na poziomie plików w systemie Windows
- Ulepszenia dotyczące aplikacji
 - Możliwość wysyłania aktualizacji PowerProtect Data Manager 19.10 do wszystkich agentów z centralnego serwera PowerProtect Data Manager, co ogranicza konieczność wykonywania pojedynczych aktualizacji ręcznych
 - Obsługa hostów/agentów w przypadku wielu nazw domen FQDN

Integracja ze Smart Scale

- PowerProtect Data Manager jako aplikacja do tworzenia kopii zapasowych dla Smart Scale

- [Smart Scale — prezentacja dla klientów](#)

Cyber Recovery i Cyber Sense

- Obsługa przesyłania danych do archiwum z drzew MTtree z zachowaniem zgodności z blokadą retencji
- Zwiększenie wydajności skanowania PowerProtect Data Manager Exchange

Nowości w programie PowerProtect Data Manager w wersji 19.9 (wrzesień 2021 r.)

Nowoczesne przypadki użycia

- Scentralizowana ochrona bazy danych Oracle w systemie AIX, w tym obsługa agenta Oracle-RMAN-Agent dla systemu AIX 7.1
- Obsługa zaawansowanych parametrów Oracle na potrzeby dostrajania wydajności
- Kubernetes: wykorzystanie schematów strukturalnych w CRD

Przypadki użycia VMware

- **Migawki Transparent Snapshot** (główna cecha wyróżniająca) — nowa metoda tworzenia obrazów maszyn wirtualnych, która śledzi pojawiające się zmiany, eliminując opóźnienia występujące podczas tworzenia migawki. Dzięki nowej, zarządzanej wtyczce przenoszącej dane, która zmniejsza zapotrzebowanie na zewnętrzne serwery proxy, rozwiązanie PowerProtect Data Manager zapewnia pełną ochronę obrazów maszyn wirtualnych dla wszystkich systemów o znaczeniu krytycznym dla firmy.
- Zmiana ustawień sieciowych maszyn wirtualnych podczas przywracania ułatwia i przyspiesza aktualizowanie tych ustawień.
- Obsługa ochrony maszyn wirtualnych PowerProtect Data Manager dla silnika Google Cloud VMware Engine

W chmurze

- Cloud DR z obsługą programu PowerProtect Data Manager dla środowisk sieci prywatnych na platformach AWS i Azure
- Prostsza instalacja rozwiązań Data Manager i APEX Protection Storage w Azure Marketplace
- Kopiowanie migawki do APEX Protection Storage w Azure w celu obniżenia kosztów pamięci masowej

Integracja pamięci masowej

- **Dynamiczna ochrona pamięci masowej NAS** (główna cecha wyróżniająca) — automatyzuje i optymalizuje ochronę infrastruktury NAS, zapewniając prosty, nowoczesny sposób zabezpieczania systemów NAS.

Możliwości serwisowania, dostępność, TCE

- Ulepszenia dotyczące zadań i serwisowania, w tym:
 - Obsługa anulowania zadań ochrony i przywracania w przypadku wszystkich agentów aplikacji
 - Obsługa anulowania różnych zadań (zgodność, przechowywanie ad hoc, eksport itp.)
 - Możliwość pobierania kompleksowych dzienników
 - Kompleksowe dzienniki na potrzeby całościowego debugowania
 - Obsługa usuwania zasobów i źródeł zasobów
 - Ulepszone komunikaty o błędach (EEMI)
 - Ulepszona obsługa zarządzania cyklem życia pakietów aktualizacji
 - Obsługa tworzenia kopii zapasowych serwera przez DDBoost
 - Nowe natywne widoki zasobów dla SQL
- Cyber Recovery
- Obsługa scentralizowanych konfiguracji dziennika systemowego
 - Interfejsy API REST w portalu Dell Marketplace

Dodatkowe ulepszenia

- Wszystkie dokumenty interfejsu API są dostępne na stronie <http://developer.dell.com>
- Zezwalanie na edytowanie wyłączonych zasad ochrony
- Obsługa funkcji Smart Scale dla pul systemów
- Udostępnienie rozwiązania Hadoop do ochrony bazy danych HBASE wdrożonej w klastrze Hadoop.

Wprowadzenie wersji PowerProtect Data Manager Essentials (czerwiec 2021 r.)

PowerProtect Data Manager Essentials to oprogramowanie do ochrony danych, które udostępnia ten sam zestaw funkcji co PowerProtect Data Manager (Plus), ale ze względu na pułap cenowy i ograniczenia dotyczące pojemności/procesorów jest przeznaczone dla firm średniej wielkości. Częścią nowej oferty jest nowa usługa wdrożeniowa ProDeploy. ProDeploy dla programu PowerProtect Data Manager Essentials to pakiet usług wdrażania składników oprogramowania, który jest dostosowany do najczęstszych przypadków użycia rozwiązania PowerProtect Data Manager Essentials. Więcej informacji o nowej usłudze można znaleźć na [tej stronie](#).

Nowości w programie PowerProtect Data Manager w wersji 19.8 (maj 2021 r.)

W chmurze

- Integracja z programem [PowerProtect Cloud Snapshot Manager](#) — oprogramowanie PowerProtect Data Manager udostępnia podsumowanie informacji i alertów z narzędzia PowerProtect Cloud Snapshot Manager
- Zintegrowany przepływ pracy wdrażania produktów PowerProtect Data Manager + APEX Protection Storage AWS z AWS Marketplace zapewnia lepszą i prostszą obsługę od samego początku
- Cloud DR — zgodność z rygorystycznymi standardami programu AWS Storage Competency

VMware

- Certyfikaty VMware: VMC, vSAN/vSphere, VCF
- Certyfikat Data Manager 19.6: VMware Ready w zakresie rozwiązań vSphere/vSAN 6.7.x i 7.0
- Certyfikat Data Manager 19.7: VMware Ready w zakresie rozwiązań vSphere/vSAN 7.0 U2; VMware Cloud on AWS M14
- Kwalifikacja vSphere 7.0 U1 i U2 z obsługą programu Data Manager
- Data Manager 19.7: certyfikat VMware z obsługą rozwiązania VCF 4.2
- Funkcja przywracania skompresowanych PowerProtect Data Domin w rozwiązaniu vProxy skraca docelowy czas odzyskiwania
- Wyszukiwanie i przywracanie plików w ramach wielu maszyn wirtualnych

Nowoczesne przypadki użycia

- Ochrona kontenerów Kubernetes: obsługa ogólnie dostępnej wersji interfejsu Container Storage Interface dla migawek
- Ulepszenia dotyczące narzędzia vProtect
 - RBAC — wstępnie zdefiniowane role administratora/operatora
 - Pełne i przyrostowe kopie zapasowe plików Nutanix (AFS) ze śledzeniem zmienionych plików
 - Zarządzanie migawkami dla Ceph RBD
 - Udoskonalenia integracji interfejsów użytkownika oVirt, RHV i OLVM
 - Ulepszona prezentacja danych
 - Przewodnik po konfiguracji tworzenia kopii zapasowych baz danych oVirt, RHV i OLVM
- Tworzenie kopii zapasowych Hadoop i przywracanie list ACL atrybutów rozszerzonych oraz zaszyfrowanych zestawów danych
- Obsługa wielu strumieni w przypadku tworzenia kopii zapasowych opartych na plikach w systemach Windows i Linux
- Scentralizowane przywracanie SQL App Direct wielu baz danych z poziomu interfejsu użytkownika programu PowerProtect Data Manager

Cyber Recovery

- Magazyn Cyber Recovery w formacie urządzenia PowerProtect z serii DP
- Wykrywanie anomalii w obciążeniach roboczych programu PowerProtect Data Manager
- Cyber Recovery Telemetry — bezpieczna telemetria oparta wyłącznie na poczcie e-mail
- Obsługa wielu urządzeń wirtualnych DDVE w ramach rozwiązania Cyber Recovery na platformie AWS

Operatywność, dostępność, TCE (dodatkowe ulepszenia)

- Ulepszenia dotyczące reguł zasad — refaktoryzacja interfejsu użytkownika zasad pozwala uwzględnić wiele operacji w jednej regule ochrony
- Lepsza widoczność zadań na potrzeby śledzenia na poziomie zasobów
- Identyfikacja zarządzania dostępem — dodano zasoby wielu tożsamości (LDAP/AD) w celu ułatwienia uwierzytelniania
- Narzędzie SupportAssist usprawnia korzystanie z pomocy technicznej
- Automatyczne przywracanie programu PowerProtect Data Manager i węzła wyszukiwania w przypadku awarii

Integracja z CloudIQ (kwiecień 2021 r.)

Integracja oprogramowania PowerProtect Data Manager z CloudIQ umożliwia proaktywne monitorowanie oraz analizę predykcijną i wgląd w dane w celu ograniczenia ryzyka, planowania z wyprzedzeniem i poprawy produktywności dzięki skróceniu czasu rozwiązywania problemów. Użytkownicy rozwiązania PowerProtect Central zostaną przekierowani do CloudIQ. Dodatkowe informacje można znaleźć w sekcji „Monitorowanie i analiza oparta na chmurze” w tym dokumencie.

Nowości w programie PowerProtect Data Manager w wersji 19.7 (luty 2021 r.)

W chmurze

- Wdrażanie rozwiązania Data Manager na platformie Google Cloud. Łatwe wdrożenie z wykorzystaniem Google Marketplace. Obsługa technologii SQL, Oracle, SAP HANA i GKE
- Cloud Snapshot Manager: kopiowanie migawek AWS do urządzenia wirtualnego PowerProtect DDVE
- Odtwarzanie po awarii w chmurze: ochrona i odzyskiwanie większych maszyn wirtualnych oraz ochrona regionów Azure Government

Nowoczesne przypadki użycia

- Ochrona platformy Kubernetes
 - Ochrona klastrów gościa Kubernetes w VMware Tanzu

- Ochrona zasobów PaaS OpenShift
- Ochrona rozwiązania GKE działającego na platformie Google Cloud
- Ochrona systemów Hadoop (za pośrednictwem RPQ: ochrona większej liczby plików i większych klastrów)
- Ulepszenia dotyczące narzędzia vProtect: obsługa blokady przechowywania DD, wtyczka interfejsu użytkownika OpenStack, raportowanie obciążeń zwrotnych w interfejsie vProtect.

Przypadki użycia VMware

- Szczegółowe włączanie/wyłączanie stanu spoczynku na poziomie środowiska VMware / zasobu
- Automatyzacja konfiguracji ochrony VCF

Cyber Recovery

- Wdrażanie magazynu Cyber Recovery w AWS
- Obsługa DLM w magazynie Cyber Recovery (za pośrednictwem RPQ)
- Dzielne raporty o stanie zadań

Ulepszanie kontaktów z klientami

- Ulepszenia w zakresie operatywności zadań
- Elastyczne opcje harmonogramu w ramach zasad

Nowości w programie *PowerProtect Data Manager* w wersji 19.6 (październik 2020 r.)

- Wdrażanie oprogramowania PowerProtect Data Manager na platformach Azure, Azure Government i AWS GovCloud w celu ochrony obciążeń roboczych w chmurze
- Zarządzanie pamięcią masową na podstawie zasad dla maszyn wirtualnych VMware
- Ochrona zasobów VMware Cloud Foundation
- Zgodna z aplikacjami ochrona zasobów PostgreSQL i Cassandra na platformie Kubernetes bez użycia agentów
- Ochrona klastrów Kubernetes w środowiskach wielochmurowych
- Tworzenie kopii zapasowych zasobów na poziomie klastra Kubernetes
- Scentralizowane przywracanie danych SQL z uwzględnieniem aplikacji
- Rozszerzony monitoring SaaS
- Zwiększona odporność na awarie
- Obsługa rozwiązania vRA 8.2

Nowości w programie PowerProtect Data Manager w wersji 19.5

Ochrona danych obciążeń roboczych na platformie AWS

- Wdrażanie oprogramowania PowerProtect Data Manager na platformie AWS dzięki automatyzacji z AWS Marketplace w celu ochrony obciążeń roboczych o znaczeniu krytycznym w chmurze

Prostsze korzystanie z ochrony danych w chmurze hybrydowej

- Kompleksowa ochrona danych w chmurze (retencja długoterminowa, odzyskiwanie danych po awarii w chmurze, tworzenie kopii zapasowych w chmurze i tworzenie kopii zapasowych w scenariuszach dotyczących chmury) w prosty i elastyczny sposób w ramach subskrypcji
- Rozszerzona obsługa monitorów maszyn wirtualnych za pomocą narzędzia [vProtect](#), w tym Nutanix, oVert, ProxMox, Xen, Openstack, Oracle VM, Redhat, KVM, XCP-NG i Oracle Linux
- Ochrona środowisk Microsoft Exchange
- Obsługa pamięci masowej ochrony urządzenia Integrated Data Protection Appliance

Kubernetes

- Spójne z aplikacjami kopie zapasowe baz danych MySQL i MongoDB działających w środowisku Kubernetes
- Odzyskiwanie danych w alternatywnym klastrze Kubernetes

Ulepszona funkcja raportowania oparta na SaaS

- Podsumowanie ochrony zasobów z ostatnich 24 godzin
- Widok historycznych działań związanych z ochroną i szczegóły dotyczące każdego chronionego zasobu
- Podsumowanie ochrony zasobów w graficznym widoku aktualnych zasad dotyczących zasobu
- Podsumowanie zasobów z najczęstszymi naruszeniami z wyszczególnieniem zasobów z największą liczbą kolejnych nieudanych operacji utworzenia podstawowej kopii zapasowej
- Raport z audytu konsolidujący dzienniki kontrolne z wystąpienia PowerProtect Data Manager w środowisku

Czym jest oprogramowanie PowerProtect Data Manager?

Czym jest oprogramowanie Dell PowerProtect Data Manager?

PowerProtect Data Manager to rozwiązanie do ochrony danych nowoczesnych wielochmurowych obciążeń roboczych, w tym aplikacji bazodanowych, maszyn

wirtualnych, kontenerów Kubernetes i systemów plików w środowisku lokalnym i w chmurze. PowerProtect Data Manager umożliwia administratorom baz danych samoobsługową ochronę i odzyskiwanie danych za pośrednictwem narzędzia Application Direct (dawniej DDBoost for Enterprise Applications). Rozwiązanie PowerProtect Data Manager zapewnia płynną integrację z VMware, ochronę maszyn wirtualnych i zaawansowane odzyskiwanie z wykorzystaniem wydajnych wirtualnych serwerów proxy. PowerProtect Data Manager udostępnia też usługi w zakresie ochrony danych m.in. w zakresie zgodności z przepisami, nadzoru, bezpieczeństwa, widoczności i analizy danych objętych zarządzaniem.

Czy PowerProtect Data Manager zastępuje istniejące produkty firmy Dell do ochrony danych?

Nie. PowerProtect Data Manager uzupełnia dotychczasową ofertę Data Protection. Oprogramowanie PowerProtect Data Manager nie zastępuje istniejących produktów DP (NetWorker, Avamar, RecoverPoint for Virtual Machines, Cloud Snapshot Manager itp.). Klienci potrzebują rozwiązań w zakresie ochrony, które obsługują ich zmieniające się środowiska IT. Rozwiązanie PowerProtect Data Manager należy oferować w następujących przypadkach:

- Klient nie korzysta z żadnych rozwiązań Dell w zakresie ochrony danych.
- Klient korzysta z PowerProtect Data Domain, ale nie ma pakietu Data Protection Suite (Avamar i NetWorker).
- Klient korzysta z PowerProtect Data Domain i pakietu Data Protection Suit (do odświeżenia lub instalacji starszej wersji).
- Współistnienie: gdy klient ma produkty Avamar i musi również chronić nowoczesne obciążenia robocze, np. Kubernetes. Współistnienie z rozwiązaniem Data Protection Central.

Jakie są najważniejsze cechy i zalety produktu PowerProtect Data Manager z punktu widzenia klienta?

Atrybut	Korzyści dla klientów
Rozwiązanie zdefiniowane programowo	Oprogramowanie, które współdziała bezpośrednio z fizycznymi lub wirtualnymi urządzeniami Dell PowerProtect
Automatyzacja i aranżacja	Automatyczne wykrywanie i ochrona baz danych, maszyn wirtualnych, systemów plików i kontenerów Kubernetes
Optymalizacja pod kątem wielu chmur	Obsługa wszystkich scenariuszy ochrony danych w chmurze: retencja długoterminowa, odtwarzanie po awarii, zapisywanie kopii zapasowych w chmurze i tworzenie ich w ramach chmury
Samoobsługa	Właściciele danych mogą tworzyć kopie zapasowe i przywracać dane bezpośrednio z natywnych interfejsów aplikacji
Scentralizowany nadzór i zarządzanie	Ograniczenie ryzyka i zapewnienie zgodności z umowami SLA i SLO

Oparta na chmurze analityka i monitorowanie	Integracja z Dell APEX AIOps zapewnia telemetrię, uczenie maszynowe i analizę predykcyjną w celu proaktywnego podejmowania działań i szybszego rozwiązywania problemów.
Skuteczna ochrona	Ochrona danych bezpośrednio na urządzeniach PowerProtect
Nowoczesna architektura oparta na usługach	Model ciągłego wprowadzania innowacji i ulepszeń

Jakie obciążenia robocze są obsługiwane przez program PowerProtect Data Manager?

PowerProtect Data Manager umożliwia obsługę następujących obciążeń roboczych:

- Bazy danych: Oracle, SQL, SAP HANA, Exchange
- Obciążenia natywne dla chmury: kontenery Kubernetes.
- Ochrona, odzyskiwanie i replikacja maszyn wirtualnych.
- Systemy plików: Windows i Linux
- PowerProtect Data Manager może chronić środowiska Oracle, SQL, SAP HANA i Kubernetes oraz maszyny wirtualne działające w VMC.
- Licencja na oprogramowanie PowerProtect Data Manager umożliwia aktywację narzędzia Cloud Snapshot Manager — rozwiązania SaaS, które ułatwia ochronę krytycznych obciążeń roboczych w chmurze publicznej poprzez wykorzystanie podstawowej technologii migawek dostawców chmury bez konieczności instalacji lub posiadania infrastruktury.
- Uwaga: obciążenia robocze Hadoop, DB2, Exchange, SAP Hana i SAP for Oracle są obsługiwane przez funkcje Application Direct i Storage Direct Protection programu PowerProtect Data Manager.

Czy planowana jest obsługa większej liczby obciążeń w przyszłych wersjach?

Tak (jeśli klient potrzebuje wsparcia w zakresie obciążenia roboczego, które nie jest obecnie obsługiwane, należy poprosić o spotkanie z działem zarządzania produktami).

Czy w przypadku programu PowerProtect Data Manager jest wymagana pamięć masowa Dell Protection Storage?

Tak. PowerProtect Data Domain jest wymaganym celem dla PowerProtect Data Manager. Alternatywnie urządzenie PowerProtect Data Manager Appliance jest również dostępne jako urządzenie zintegrowane.

Czy oprogramowanie PowerProtect Data Manager działa w chmurze?

Tak. Coraz więcej firm przyjmuje strategię wielochmurową, dlatego wykorzystanie wspólnego rozwiązania do ochrony danych w infrastrukturze lokalnej i chmurze publicznej umożliwi im osiągnięcie efektywności operacyjnej i obniżenie kosztów. W przypadku przedsiębiorstw, które mają obciążenia robocze działające na platformach

AWS, Azure i Google Cloud oraz potrzebują funkcji samoobsługowego tworzenia kopii zapasowych i przywracania danych za pomocą aplikacji firmowych, rozwiązanie PowerProtect Data Manager zapewnia ochronę danych obciążeń roboczych w środowiskach AWS, AWS GovCloud, Azure, Azure Government i Google Cloud. Właściciele danych i administratorzy mogą wdrożyć rozwiązanie PowerProtect Data Manager w tych chmurach dzięki funkcjom automatyzacji z AWS, Azure i Google Cloud Marketplace w celu ochrony obciążeń roboczych o znaczeniu krytycznym w chmurze. PowerProtect Data Manager umożliwia ochronę tradycyjnych obciążeń roboczych, w tym Oracle, SQL, SAP HANA i systemów plików, a także aplikacji chmurowych działających w kontenerach Kubernetes lub maszynach wirtualnych w chmurze VMware Cloud (VMC).

Łatwy w instalacji i wdrożeniu z poziomu platform AWS, Azure i Google Cloud Marketplace program PowerProtect Data Manager oraz rozwiązanie APEX Protection Storage zapewniają poziom wydajności i deduplikacji wyższy niż u konkurentów na tym rynku.

Kim są klienci docelowi?

Klienci, którzy nie korzystają z rozwiązania Dell Data Protection.

Klient korzysta z PowerProtect Data Domain, ale nie ma pakietu Data Protection Suite (Avamar i NetWorker).

Klient korzysta z PowerProtect Data Domain i pakietu Data Protection Suite (do odświeżenia lub instalacji starszej wersji).

Czy produkty Avamar i NetWorker są częścią oprogramowania PowerProtect Data Manager lub są przez nie obsługiwane?

Nie. Rozwiązania Avamar i NetWorker są częścią pakietu Data Protection Suite i są przez niego obsługiwane ([zobacz zestaw narzędzi w pakiecie Data Protection](#)).

Funkcje oprogramowania PowerProtect Data Manager

Jakie funkcje oferuje rozwiązanie PowerProtect Data Manager?

- Interfejs administracyjny do automatyzacji, aranżacji i zarządzania.
- Oparta na chmurze analityka i monitorowanie za pośrednictwem Dell APEX AIOps.
- Migawki Transparent Snapshot upraszczają tworzenie kopii zapasowych obrazów maszyn wirtualnych, zapewniając niemal zerowy wpływ na maszyny wirtualne oraz dostępność wszystkich maszyn wirtualnych w odpowiedniej skali bez zakłóceń w działalności.
- Replikacja maszyn wirtualnych — szybka replikacja i odzyskiwanie w środowiskach zwirtualizowanych.
- Storage Direct Protection – bezpośrednia ścieżka między pamięcią masową Dell poziomu 1 i urządzeniami z serii Data Domain zwiększa wydajność zarówno tworzenia kopii zapasowych, jak i odzyskiwania danych.

- Dynamiczna ochrona NAS — automatyzacja i optymalizacja ochrony infrastruktury NAS w celu osiągnięcia lepszych poziomów SLA dzięki prostemu, wydajnemu zarządzaniu tworzeniem kopii zapasowych i odzyskiwaniem danych zasobów NAS.
- Application Direct – samoobsługowe tworzenie kopii zapasowych i odzyskiwanie danych między aplikacjami i PowerProtect Data Domain.
- Ochrona danych w chmurze — kopie zapasowe zapisywane w chmurze i wewnętrzne kopie zapasowe zasobów chmurowych, retencja długoterminowa i odtwarzanie po awarii w chmurze.
- Ochrona oparta na SaaS za pośrednictwem narzędzia [PowerProtect Cloud Snapshot Manager](#), które umożliwia klientom wykrywanie, aranżowanie i automatyzację ochrony obciążeń roboczych w wielu chmurach w oparciu o zasady sprawnego tworzenia kopii zapasowych i odtwarzania po awarii.

PowerProtect Data Manager

Jaka jest nadrzędna wartość rozwiązania Dell PowerProtect Data Manager?

Dell PowerProtect Data Manager zapewnia ochronę danych w nowoczesnym centrum przetwarzania danych. Zapewnia zarówno samoobsługową ochronę danych, jak i centralne środowisko nowoczesnego, prostego i elastycznego tworzenia kopii zapasowych w organizacjach w trakcie transformacji cyfrowej.

Data Manager zapewnia klientom następujące możliwości:

- Automatyzacja przydzielania PowerProtect Data Domain, która pozwala administratorom baz danych na obsługę obiektów docelowych ochrony w postaci usługi.
- Wykrywanie i katalogowanie kopii zapasowych wykonywanych w sposób samoobsługowy przez administratorów IT (administratorów baz danych) w celu monitorowania zgodności ochrony z celami firmy (tj. RPO).
- Niezawodna dostępność wszystkich maszyn wirtualnych niezależnie od skali bez zakłóceń w działalności.
- Automatyzacja i optymalizacja ochrony infrastruktury NAS.
- Samoobsługowa ochrona danych dzięki skonsolidowanemu nadzorowi w celu optymalizacji działań związanych z tworzeniem kopii zapasowych i zapewnienia lepszego RTO w przypadku baz danych. Wymuszanie tworzenia kopii zapasowych obrazów maszyn wirtualnych dla tych baz danych za pomocą filtrów dynamicznych.
- Umożliwienie administratorom ds. zgodności tworzenia kopii zapasowych zasobów maszyn wirtualnych, SQL, Oracle i systemów plików.
- Wprowadzenie zasad ochrony w celu automatycznego tworzenia kopii zapasowych, replikacji i tworzenia warstw różnych obciążeń roboczych.

- Obsługa wszystkich scenariuszy ochrony danych w chmurze: retencja długoterminowa, odtwarzanie po awarii w chmurze, tworzenie kopii zapasowych w chmurze i przechowywanie wewnętrznych kopii zapasowych w chmurze.

W jaki sposób rozwiązanie PowerProtect Data Manager umożliwia ochronę danych?

PowerProtect Data Manager zapewnia ochronę danych, ułatwiając tworzenie zasad konfiguracyjnych replikację kopii zapasowych, a nawet tworzenie warstw w chmurze zgodnie z wybranym harmonogramem. Po skonfigurowaniu umów o poziomie usług zgodnych z potrzebami organizacji program PowerProtect Data Manager powiadamia o tym, czy są one przestrzegane.

W jaki sposób rozwiązanie PowerProtect Data Manager umożliwia transformację IT?

Uzupełniając samoobsługowy model tworzenia kopii zapasowych aplikacji, program PowerProtect Data Manager rozszerza paradygmat ochrony o centralne planowanie kopii zapasowych baz danych dla agenta SQL Boost, agenta Oracle RMAN, maszyn wirtualnych i systemów plików z poziomu interfejsu użytkownika PowerProtect Data Manager. Dzięki temu zespół ds. kopii zapasowych może centralnie zarządzać harmonogramami tworzenia pełnych, przyrostowych, różnicowych oraz opartych na dziennikach kopii zapasowych, jednocześnie ułatwiając migrację zespołowi ds. administracji bazami danych, który może chcieć korzystać z funkcji Application Direct.

Jaki problem rozwiązuje program PowerProtect Data Manager?

PowerProtect Data Manager zapewnia organizacjom proste, szybkie i skuteczne sposoby ochrony danych.

- Administrator bazy danych może zaplanować tworzenie kopii zapasowych własnych zasobów.
- Administrator kopii zapasowych może monitorować kopie zapasowe wykonywane przez administratorów baz danych i planować tworzenie własnych kopii zapasowych.

PowerProtect Data Manager ułatwia przywracanie danych z kopii zapasowej za pośrednictwem funkcji Live VM albo na alternatywnej lub oryginalnej maszynie wirtualnej. Pulpity informacyjne ułatwiają użytkownikowi śledzenie stanu środowiska ochrony danych i dostarczają powiadomienia o wszelkich problemach. Dzięki globalnej deduplikacji zapotrzebowanie na sieć i pamięć masową jest znacznie mniejsze, a technologia DD Boost zapewnia najwyższą szybkość tworzenia kopii zapasowych.

Jakie są korzyści ze skonsolidowanego nadzoru za pomocą rozwiązania Dell PowerProtect Data Manager?

Dzięki możliwości zarządzania zdecentralizowanymi operacjami ochrony, które zużywają zasoby urządzeń PowerProtect Data Domain, administratorzy kopii zapasowych mogą przekazać złożone obowiązki związane z tworzeniem kopii zapasowych innym członkom zespołu, aby poświęcić zaoszczędzony czas na innowacyjne działania. Administratorzy ds. kopii zapasowych lub zgodności z przepisami mogą skonfigurować program PowerProtect Data Manager w celu proaktywnego definiowania celów dotyczących poziomu usług i reaktywnego rozwiązywania potencjalnych problemów ze zgodnością ochrony z przepisami.

Czym jest funkcja Transparent Snapshot?

Funkcja migawek Transparent Snapshot dostępna w programie PowerProtect Data Manager od wersji 19.9 to nowy sposób ochrony i tworzenia kopii zapasowych maszyn wirtualnych VMware na dużą skalę bez kompromisów w zakresie opóźnień, kosztów, skalowalności, wydajności i złożoności. Tradycyjne metody nie pozwalają przewyciężyć problemów związanych z zakłóceniami w działalności podczas tworzenia kopii zapasowych maszyn wirtualnych, ale oprogramowanie Transparent Snapshots usuwa te przeszkody, przez co wcześniejsze rozwiązania tego typu stają się przestarzałe. Upraszczając i automatyzując tworzenie kopii zapasowych na poziomie obrazu maszyny wirtualnej przy ograniczeniu wymagań dotyczących infrastruktury, organizacje mogą zapewnić dostępność danych maszyn wirtualnych skuteczniej i wydajniej niż kiedykolwiek wcześniej. Funkcja Transparent Snapshots umożliwi szybsze tworzenie kopii zapasowych i zmniejszenie opóźnień maszyn wirtualnych.

Co to jest Storage Direct Protection?

Technologia Storage Direct Protection, dostępna tylko w programie Dell PowerProtect Data Manager, to kompleksowe rozwiązanie przeznaczone do szybkiego, wydajnego i bezpiecznego tworzenia kopii zapasowych i odzyskiwania danych w wielu klastrach i migawkach lokalnych. Oferuje on:

- **Szybkie tworzenie kopii zapasowych i odzyskiwanie danych:** minimalizacja utraty danych dzięki krótszym celom Recovery Point Objective (RPO), za sprawą funkcji szybkiego tworzenia kopii zapasowych i odzyskiwania danych w różnych środowiskach.
- **Skuteczna ochrona ekosystemu:** bezproblemowe przywracanie na oryginalne lub alternatywne platformy pamięci masowej firmy Dell, obsługujące szerszy ekosystem przy jednoczesnym zapewnieniu skutecznej ochrony danych.
- **Zapewnienie integralności danych:** ochrona danych dzięki funkcjom niezmienności i cybersejfu, który zapewnia solidną integralność danych.
- **Proste operacje:** scentralizowane zarządzanie i orkiestracja, a także automatyczne wykrywanie i ochrona nowych woluminów, które upraszczają codzienne operacje.
- **Obsługa wielu chmur:** większa elastyczność dzięki funkcjom replikacji PowerProtect Data Domain i podziału na warstwy w chmurze, które zapewniają bezproblemową integrację ze środowiskami wielochmurowymi.

Co to jest dynamiczna ochrona NAS?

Funkcja dynamicznej ochrony NAS, dostępna w programie PowerProtect Data Manager w wersji 19.9, to rozwiązanie, które odpowiada na potrzeby klientów w zakresie ochrony ich zmieniających się środowisk NAS. Dynamiczna ochrona NAS działa niezależnie od pamięci masowej, automatycznie wykrywa zasoby NAS, tworzy przyrostowe kopie zapasowe bez ograniczeń czasowych, zapewnia automatyczne i dynamiczne dzielenie zasobów NAS z równoważeniem obciążenia oraz oferuje automatyczne skalowanie zasobów obliczeniowych w celu optymalizacji wydajności. Dynamiczna ochrona NAS umożliwia szybsze tworzenie kopii zapasowych i przywracanie.

Co to jest wykrywanie anomalii?

Wykrywanie anomalii wykorzystuje uczenie maszynowe do szybkiego identyfikowania podejrzanej aktywności podczas tworzenia kopii zapasowych w środowisku produkcyjnym, zapewniając bezpieczeństwo i integralność przy minimalnym wpływie na zasoby bez dodatkowych kosztów.

- **Kompleksowa** ocena metadanych kopii zapasowych w celu zapewnienia integralności infrastruktury cyfrowej i zwiększenia spójności operacyjnej
- **Prewencyjne** wykrywanie anomalii zapewnia szybki i bezpieczny wgląd w potencjalne zagrożenia bezpieczeństwa
- **Proaktywne** uczenie maszynowe analizuje wzorce w celu wykrycia podejrzanej aktywności, broniąc przed zagrożeniami, zanim się one rozwiną.
- **Lekkie** wykrywanie lokalne w programie PowerProtect Data Manager

Optymalizacja pod kątem wielu chmur

Co to jest tworzenie warstw w chmurze PowerProtect?

Klienci mogą przenosić kopie zapasowe do warstwy chmury po upływie określonego czasu. Dzięki temu można w pełni wykorzystać inwestycje w lokalną pamięć masową do ochrony przy jednoczesnym zachowaniu zgodności z przepisami i utrzymaniu nadzoru oraz przechowywania kopii zapasowych w chmurze.

Funkcja PowerProtect Cloud Tier umożliwia tworzenie warstw danych objętych długoterminową ochroną w pamięci masowej w chmurze dostarczanej przez wybranego dostawcę rozwiązań chmurowych. Klient może określić, jak długo dana kopia zapasowa zasobów powinna być przechowywana lokalnie, a rozwiązanie PowerProtect Data Manager automatycznie przeniesie pliki po upływie tego okresu.

Jakie chmury są obsługiwane przez funkcję PowerProtect Cloud Tier?

Dell ECS, Amazon Web Services (AWS), Microsoft Azure, IBM Cloud, Google Cloud Platform oraz Alibaba.

Czy PowerProtect Data Manager chroni obciążenia robocze w chmurze?

Klienci mogą korzystać z rozwiązania PowerProtect Data Manager na platformach AWS, AWS GovCloud, Azure, Azure Government i Google Cloud, aby chronić następujące obciążenia robocze: SQL, Oracle, SAP HANA, klastry Kubernetes, a także maszyny wirtualne działające w VMC.

Czy program PowerProtect Data Manager udostępnia funkcję Cloud Disaster Recovery?

Tak, ta funkcja jest dostępna w programie PowerProtect Data Manager 19.2 i nowszych wersjach.

Czym jest funkcja Cloud Disaster Recovery?

Cloud Disaster Recovery (Cloud DR) umożliwia przedsiębiorstwom kopiowanie chronionych maszyn wirtualnych ze środowisk PowerProtect Data Manager do obiektowej pamięci masowej w chmurze publicznej oraz aranżowanie zautomatyzowanych testów DR, przełączania awaryjnego i przywracania obciążeń roboczych warstwy 2 do i z chmury w przypadku awarii. Rozszerzenie istniejącej ochrony danych z lokalizacji klienta na chmurę zapewnia znajome środowisko

użytkownika, a tym samym wymaga minimalnych umiejętności i szkoleń. Dodatkowymi zaletami funkcji Cloud DR są minimalne obciążenia chmury podczas rutynowych operacji i uporządkowane odzyskiwanie danych.

Jakie chmury publiczne są obsługiwane przez funkcję Cloud Disaster Recovery?

Ochrona za pomocą funkcji Cloud DR jest obsługiwana w przypadku usług przechowywania obiektów AWS i Azure.

Cloud DR obsługuje odzyskiwanie danych do natywnego wystąpienia chmury oraz bezpośrednie odzyskiwanie do środowiska VMware Cloud on AWS lub lokalnego rozwiązania vCenter.

Jakie są zalety funkcji Cloud Disaster Recovery?

Opłacalna ochrona chmury w chmurze — wykorzystanie obiektowej pamięci masowej i minimalnej ilości zasobów obliczeniowych w chmurze podczas bieżącej ochrony oraz używanie dodatkowych zasobów obliczeniowych w przypadku odzyskanych wystąpień na żądanie, gdy wymagane jest przełączanie awaryjne.

- Zapisywanie dodatkowych kopii maszyn wirtualnych w magazynie obiektów w chmurze.
- Przywracanie danych do wystąpień chmurowych, VMware Cloud on AWS lub z powrotem do lokalnego środowiska vCenter za pomocą trzech kliknięć.
- Przywracanie dwoma kliknięciami środowisk po awarii w chmurze publicznej AWS lub Azure po zdarzeniu przełączania awaryjnego.

Application Direct

Co to jest funkcja Application Direct?

Application Direct umożliwia właścicielom danych tworzenie kopii zapasowych i przywracanie danych bezpośrednio z aplikacji natywnych na urządzenia serii PowerProtect Data Domain, APEX Protection Storage i DP lub Integrated Data Protection Appliance, podczas gdy PowerProtect Data Manager umożliwia nadzór i zarządzanie.

Na czym polega kluczowa zaleta funkcji Application Direct?

- **Integracja aplikacji:** Application Direct wykorzystuje macierzysty interfejs zarządzania w aplikacjach, aby umożliwić ich właścicielom przechowywanie danych bezpośrednio w pamięci masowej do ochrony.
- **Zoptymalizowana mobilność danych:** Application Direct używa rozwiązania DD Boost jako modułu przenoszenia danych. Pozwala to na rozproszone przetwarzanie segmentów na serwerze aplikacji i wysyłanie przez sieć tylko unikatowych danych do urządzeń PowerProtect Data Domain, co umożliwia szybsze tworzenie kopii zapasowych.

Jakie agenty aplikacji są dołączone do programu PowerProtect Data Manager?

- Oracle: właściciele aplikacji mogą szybciej tworzyć kopie zapasowe bezpośrednio przy użyciu Oracle RMAN.

- Microsoft SQL Server: właściciele aplikacji mogą szybciej tworzyć kopie zapasowe bezpośrednio z programu Microsoft SQL Server Management Studio.
- MS Exchange, systemy plików (Windows i Linux) oraz SAP HANA są obsługiwane za pomocą rozwiązania PowerProtect Data Manager.
- Tworzenie kopii zapasowych i odzyskiwanie danych produktów SAP, Microsoft Exchange i IBM DB2 jest obsługiwane przez Application Direct, jednak program PowerProtect Data Manager nie umożliwia jeszcze zarządzania tymi operacjami. Obsługa tych aplikacji zostanie wprowadzona w kolejnej wersji.

Agent systemu plików

Co to jest narzędzie Application Direct File System Agent?

Podobnie jak agenty aplikacji narzędzie Application Direct File System Agent dodaje możliwość ochrony systemów plików na hostach Windows i Linux.

Administrator kopii zapasowych lub systemu plików może bezpośrednio tworzyć kopie zapasowe systemów plików lub przywracać je z PowerProtect Data Domain a pośrednictwem programu PowerProtect Data Manager albo za pomocą poleceń samoobsługowych kopii zapasowej i przywracania.

Czy kopia zapasowa oparta na blokach jest obsługiwana w przypadku narzędzia File System Agent?

File System Agent obsługuje kopie zapasowe oparte na blokach w celu tworzenia kopii zapasowych i przywracania danych na poziomie obrazu.

Czy narzędzie File System Agent można zainstalować jako autonomicznego agenta do tworzenia kopii zapasowych i przywracania systemów plików bez programu Data Manager?

Nie. Narzędzie File System Agent musi być zarejestrowane w programie PowerProtect Data Manager.

Czy File System Agent obsługuje przywracanie na poziomie plików?

Tak, przywracanie na poziomie plików jest obsługiwane przy użyciu programu PowerProtect Data Manager. Funkcje indeksowania i wyszukiwania na poziomie plików będą dostępne w przyszłych wersjach.

Wtyczka systemu plików DDBoost (BoostFS)

Czy wtyczka BoostFS jest dołączona do programu PowerProtect Data Manager?

Tak

Jakie systemy operacyjne obsługuje wtyczka BoostFS?

BoostFS obsługuje systemy Windows i Linux. Informacje o konkretnych obsługiwanych wariantach systemów Linux i Windows można znaleźć w sekcji ogólnej często zadawanych pytań dotyczących Storage Direct Protection.

Obsługa produktów VMware i wirtualizacji

Jakie funkcje dotyczące produktów VMware obsługuje program PowerProtect Data Manager?

PowerProtect Data Manager zapewnia spójne z aplikacjami tworzenie kopii zapasowych i odzyskiwanie obrazów maszyn wirtualnych wielu popularnych aplikacji oraz szereg funkcji samoobsługowych dla administratorów maszyn wirtualnych. Wyszukiwanie zasobów maszyn wirtualnych ułatwia szybsze wykrywanie danych do przywrócenia.

W jaki sposób rozwiązanie PowerProtect Data Manager upraszcza i automatyzuje ochronę danych maszyn wirtualnych?

PowerProtect Data Manager to jedyne rozwiązanie zapewniające natywną integrację technologii vSphere z vCenter na potrzeby ochrony maszyn wirtualnych. Administratorzy pamięci masowej i kopii zapasowych, a także właściciele maszyn wirtualnych mają możliwość wyboru zasady dotyczącej pamięci masowej, która ma być automatycznie stosowana do każdej maszyny wirtualnej po jej utworzeniu. Ta funkcja jest również znana jako zarządzanie pamięcią masową VMware na podstawie zasad (VMware Storage Policy-Based Management — SPBM).

Co to jest natychmiastowy dostęp?

Natychmiastowy dostęp to możliwość uruchamiania wielu maszyn wirtualnych przy użyciu kopii zabezpieczającej. Dyski maszyn wirtualnych (VMDK) można montować przez sieć, aby działały na urządzeniach PowerProtect Data Domain bez konieczności przywracania danych do oddzielnego podstawowego systemu pamięci masowej.

- Unikanie kosztów związanych z produkcyjną pamięcią masową podczas przywracania kopii zapasowych maszyn wirtualnych.
- Etapowe przywracanie środowisk produkcyjnych.
- Odzyskiwanie na poziomie plików.
- Uzyskiwanie dostępu do nieprzetworzonych danych aplikacji potrzebnych do przeprowadzania analiz.
- Wykonywanie „natychmiastowego” przywracania za pomocą narzędzia VMware Storage vMotion lub interfejsu użytkownika vCenter.

Jakie są przypadki użycia funkcji Instant Access?

Funkcja Instant Access zapewnia krótki czas do uzyskania wartości w przypadku następujących pracowników działu IT:

- Zespoły DevOps mogą w ciągu kilku sekund uruchamiać aplikacje produkcyjne lub kopie na urządzeniach PowerProtect Data Domain w ramach piaskownicy testowej/deweloperskiej.
- Zespoły analityków biznesowych mogą przeprowadzać analizy na kopiach produkcyjnych baz danych aplikacji.
- Administratorzy kopii zapasowych i pamięci masowej mogą zarządzać sesjami Instant Access oraz dzierżawić, rozszerzać bądź odzyskiwać losowe zasoby we/wy zużyte w ramach natychmiastowego przywracania lub aktywności funkcji LiveVM.
- Administratorzy baz danych mogą minimalizować przestoje dzięki możliwości montowania dysków VMDK za pośrednictwem rozwiązania SQL Server Management Studio. Każda uwzględniająca aplikacje kopia zapasowa obrazu maszyny wirtualnej SQL Server automatycznie instaluje rozwiązanie SQL Server Management Studio, agenta Dell Microsoft Application Agent i narzędzie Dell ItemPoint.

Jakie są ważne różnice między kopiami zapasowymi obrazów uwzględniającymi aplikacje a kopiami zapasowymi spójnymi z aplikacjami?

Jednym z najważniejszych elementów uwzględniania zwirtualizowanych aplikacji jest obsługa unikalnych potrzeb w zakresie ochrony danych. Podstawowe rozwiązanie w zakresie obrazów maszyn wirtualnych spójnych z aplikacjami po prostu przenosi aplikacje w stan spoczynku i nic więcej.

Funkcja tworzenia kopii zapasowych PowerProtect z uwzględnieniem aplikacji wstrzykuje agenta Dell Microsoft Application Agent w ramach tego procesu. Umożliwia to tworzenie kopii zapasowych dzienników, obcinanie dzienników i instalowanie agenta ochrony rozwiązania SQL Server Management Studio, co pozwala administratorom stosować samodzielną ochronę i odzyskiwać bazy danych.

Czy program PowerProtect Data Manager obsługuje rozwiązanie vSphere?

Tak

Na czym polegają korzyści z obsługi rozwiązania vSphere?

Samoobsługa: odzyskiwanie zasobów maszyn wirtualnych bezpośrednio w środowisku vSphere.

Użytkownicy nie muszą rezygnować z preferowanego narzędzia do zarządzania ochroną danych. Narzędzia do odzyskiwania są dostępne w tym samym środowisku IDE, w którym zarządza się środowiskiem maszyn wirtualnych.

Jakie monitory maszyn wirtualnych obsługuje program PowerProtect Data Manager?

Oprócz VMware program PowerProtect Data Manager obsługuje różne monitory maszyn wirtualnych za pośrednictwem oprogramowania [vProtect](#). Dodanie narzędzia vProtect do programu PowerProtect Data Manager rozszerza zakres obsługi środowisk wirtualnych w ramach jednej oferty m.in. na produkty AWS EC2, AHV, RHEV, Oracle Virtualization Manager, Citrix Hypervisor i Xen. Administratorzy mogą zarządzać pełnymi i przyrostowymi kopiami zapasowymi i odzyskiwaniem oraz migawkami na poziomie maszyny wirtualnej, bez agentów, spójnymi z aplikacjami. Narzędzie vProtect jest

zintegrowane z PowerProtect Data Domain za pośrednictwem BoostFS do bezpośredniego odczytu/zapisu.

Co to jest wirtualizacja OpenShift?

OpenShift Virtualization to oparta na KubeVirt technologia, która rozszerza funkcjonalność Kubernetes w celu obsługi maszyn wirtualnych (VMs) i zarządzania nimi wraz ze kontenerowymi obciążeniami roboczymi w tym samym środowisku. Umożliwia to firmom wydajną integrację i obsługę starszych lub niekontenerowych aplikacji w klastrach Kubernetes.

Dlaczego klienci chcą wirtualizacji OpenShift?

Wielu klientów obsługuje aplikacje, których nie można łatwo konteneryzować, ale nadal wymagają solidnego zarządzania i ochrony danych. OpenShift Virtualization wypełnia tę lukę, umożliwiając organizacjom wykonywanie następujących zadań:

- Chronić maszyny wirtualne Linux i Windows bezpośrednio w środowiskach Kubernetes.
- Wykorzystaj standardowe podejście typu open source (KubeVirt) bez polegania na zastrzeżonych rozwiązaniach.
- Usprawnij zarządzanie, integrując maszyny wirtualne i kontenery w ujednoczonym systemie.

Rozwiązanie to jest szczególnie atrakcyjne dla branż zależnych od OpenShift, takich jak telekomunikacja, oraz dla organizacji poszukujących alternatywnych rozwiązań z zakresu monitorów maszyn wirtualnych z uwagi na kwestie związane z kosztami i licencjami.

Jakie funkcje są dostępne w wersji PowerProtect Data Manager 19.19 związanej z wirtualizacją OpenShift?

Funkcje dostępne dla wstępnej wersji obsługi wirtualizacji OpenShift w programie PowerProtect Data Manager 19.19 są następujące:

- Wstępna ochrona obrazu maszyny wirtualnej przy użyciu programu PowerProtect Data Manager zintegrowanego z Kubernetes.
- Przepływy pracy tworzenia kopii zapasowych i odzyskiwania danych o ochronie na poziomie przestrzeni nazw/woluminu trwałego (PV):
 - Przepływy pracy Przywracanie do nowego i Przywracanie do alternatywnego.
 - Obsługa zarówno systemu plików, jak i magazynu blokowego.
 - Uśpienie maszyny wirtualnej w celu zapewnienia spójności systemu plików (zamrożenie/rozmrózenie).
- Wykrywanie maszyn wirtualnych w klastrach Kubernetes.
- Ograniczona skala i wydajność.
- Blokowy moduł przenoszenia danych pamięci masowej w celu zwiększenia wydajności tworzenia kopii zapasowych.
- Mapowanie przestrzeni nazw do maszyny wirtualnej za pomocą łatwego w użyciu interfejsu użytkownika.

Jakie korzyści zapewnia ta funkcja użytkownikom?

Wirtualizacja OpenShift zapewnia znaczną wartość, w tym:

- **Kompleksowa ochrona danych Kubernetes:** Ochrona zarówno konteneryzowanych, jak i niekonteneryzowanych obciążeń roboczych w klastrach Kubernetes.
- **Kompleksowe zarządzanie:** Jedna platforma do zarządzania zarówno maszynami wirtualnymi, jak i aplikacjami Kubernetes.
- **Alternatywy dla VMware:** klienci poszukujący alternatyw dla tradycyjnych platform monitorów maszyn wirtualnych (np. VMware) mogą obniżyć koszty i zmodernizować swoją infrastrukturę.
- **Zgodność z wieloma platformami:** wykorzystanie standardowego (niezastrzeżonego) rozwiązania, które zapewnia obsługę w przyszłości i szeroką zgodność ekosystemu.

Funkcja ta zapewnia bezproblemowe zarządzanie hybrydowymi obciążeniami roboczymi i ochronę, umożliwiając organizacjom zachowanie elastyczności i konkurencyjności.

Jakie funkcje są planowane w przyszłych wersjach obsługi wirtualizacji OpenShift w programie PowerProtect Data Manager?

Przyszłe aktualizacje będą obejmować:

- Zróznicowanie maszyn wirtualnych w interfejsie użytkownika PowerProtect Data Manager.
- Zaawansowane przypadki użycia odzyskiwania, takie jak włączanie/wyłączanie zasilania, obsługa sieci i adnotacje K8s.
- Szablony aplikacji dla baz danych, takich jak MySQL, MongoDB, PostgreSQL i Cassandra.
- Rozszerzone przypadki użycia:
 - Odzyskiwanie na poziomie plików.
 - Migracja maszyn wirtualnych (odpowiednik vMotion) w Kubernetes.
 - Natychmiastowy dostęp/odzyskiwanie maszyn wirtualnych.
- Obsługa narzędzia SuSE Harvester i dodatkowych funkcji Kubernetes, takich jak migawki VolumeGroup.
- Planowanie odzyskiwania po awarii (DR) i planowanie przełączania awaryjnego/przywracania po awarii.

Te ulepszenia zapewnią jeszcze większą funkcjonalność i skalowalność, umożliwiając PowerProtect Data Manager radzenie sobie z złożonymi i dużymi wymaganiami przedsiębiorstw.

Obsługa monitora maszyn wirtualnych Hyper-V

Co to jest agent ochrony Hyper-V Protection Agent?

Hyper-V Protection Agent to nowa funkcja w programie PowerProtect Data Manager, zaprojektowana specjalnie z myślą o ochronie środowisk Hyper-V. To ulepszenie zaprojektowane od podstaw zapewnia niezawodną i odporną na cyberataki ochronę danych dla obciążeń roboczych Hyper-V.

Podstawowe korzyści

- Hyper-V Resilient Change Tracking (RCT) dla przyrostowych kopii zapasowych, które są przechowywane jako syntetyczne pełne kopie zapasowe.
- Pełne możliwości odzyskiwania maszyn wirtualnych.
- Obsługa ochrony Azure Stack HCI (obecnie Azure Local), w pełni zgodna z konfiguracjami zaplecza Hyper-V.
- Certyfikat z dodatkowymi zasadami kontroli aplikacji Dell Windows Defender (WDAC).

Jakie funkcje są dostępne podczas premiery?

Następujące funkcje będą dostępne od początkowej wersji programu PowerProtect Data Manager 19.19 z obsługą technologii Hyper-V:

- Wdrożenie serwerów Hyper-V do programu PowerProtect Data Manager.
- Wykrywanie źródeł zasobów i wykrywanie zasobów.
- Tworzenie konfiguracji i zasad.
- Pełne kopie zapasowe maszyn wirtualnych i przyrostowe kopie zapasowe.
- Pełne przywracanie obrazów maszyn wirtualnych.
- Ochrona Azure Local (dawniej Azure Stack HCI).

Jakie ulepszenia oferuje to ulepszenie w porównaniu z NetWorker lub Avamar?

Agent ochrony Hyper-V Protection Agent oferuje znaczne ulepszenia w porównaniu z NetWorker i Avamar, takie jak:

- Większa skalowalność i wydajność dzięki funkcjom takim jak multistreaming.
- Bezpośrednia obsługa funkcji Windows Defender Application Control (WDAC), która jest niedostępna w NetWorker i Avamar.
- Szybsze tworzenie kopii zapasowych i przywracanie danych dzięki wstępnej wydajności inżynierskiej wynoszącej 14 TB/h w przypadku kopii zapasowych i 1 TB/h w przypadku przywracania.
- Bezpośrednie wdrażanie i instalacja agenta typu push, bez użycia serwera proxy, tworzy środowisko niemal pozbawione agenta

Jakie są ograniczenia podczas premiery?

Chociaż początkowa wersja dodaje solidne możliwości, należy pamiętać, że istnieją pewne ograniczenia:

- Brak natychmiastowego dostępu lub zindeksowanego wyszukiwania odzyskiwania po uruchomieniu, ale te ulepszenia są na planie działania.
- Na początku brak obsługi aplikacji i baz danych SQL, z planami dodania jej w przyszłych wersjach.
- Platforma Azure Cloud Platform (APEX) dla Microsoft Azure nie jest obsługiwana.

W jaki sposób zwiększa to obsługę Azure Local (dawniej Azure Stack HCI)?

Nowy agent w pełni chroni środowiska lokalne Azure przy użyciu tej samej konfiguracji co zaplecze Hyper-V. Zapewnia to bezproblemową integrację dla organizacji korzystających z platformy Azure Local do infrastruktury lokalnej.

Dlaczego obsługa platform innych niż VMWare jest istotna?

Rozszerzenie obsługi poza VMWare ma kluczowe znaczenie, ponieważ wiele przedsiębiorstw dywersyfikuje swoje środowiska monitorów maszyn wirtualnych. Hyper-V, OpenShift Virtualization, Nutanix AHV i OpenStack/KVM to wiodące preferencje wśród klientów, którzy odchodzą od VMWare. Szersza obsługa platform zapewnia, że rozwiązanie PowerProtect Data Manager pozostaje odpowiednie na zmieniającym się rynku.

Jakie możliwości są planowane na przyszłe aktualizacje?

Przyszłe wersje programu PowerProtect Data Manager będą zawierać dodatkowe funkcje, takie jak:

- Natychmiastowy dostęp i indeksowane wyszukiwanie w celu szybszego odzyskiwania.
- Odzyskiwanie na poziomie plików bezpośrednio za pośrednictwem interfejsu użytkownika.
- Świadomość aplikacji i wsparcie dla SQL.
- Operacje na poziomie dysku, takie jak filtry wykluczania dysków kopii zapasowych i odzyskiwanie na poziomie dysku.

Storage Direct Protection

Co to jest technologia Storage Direct Protection?

Storage Direct Protection rozszerza działanie funkcji Application Direct, zapewniając bezpośrednią ścieżkę od podstawowej pamięci masowej do PowerProtect Data Domain. Umożliwia wyeliminowanie wpływu tworzenia kopii zapasowych na serwery aplikacji.

Na czym polegają korzyści dla klientów w przypadku funkcji Storage Direct Protection?

Wielu klientów nadal ma problemy ze spełnieniem wymagań dotyczących ochrony danych, zwłaszcza w przypadku aplikacji i baz danych o znaczeniu krytycznym. Technologia Storage Direct pozwala spełnić rygorystyczne wymagania dotyczące umów SLA, utrzymać wydajność i zapewnić całodobową ochronę przez cały rok.

Jakie podstawowe platformy pamięci masowej firmy Dell są obsługiwane przez funkcję Storage Direct Protection?

VMAX3, VMAX All Flash, PowerMax, PowerStore.

Które urządzenia PowerProtect Data Domain są obsługiwane przez funkcję Storage Direct Protection oprogramowania PowerProtect Data Manager?

Szczegółowe informacje można znaleźć w pełnym przewodniku po zgodności z programem Data Manager na [tej stronie](#).

Jakie aplikacje są bezpośrednio obsługiwane przez funkcję Storage Direct Protection?

Agent aplikacji umożliwia natywną obsługę następujących rozwiązań:

- EPIC w systemie Linux,
- systemy plików Linux.

Storage Direct Protection z Dell Storage

Jakie są główne zalety integracji w programie PowerProtect Data Manager?

- Zerowy wpływ na działanie hosta podczas tworzenia kopii zapasowych i odzyskiwania danych. Tworzenie kopii zapasowej działa bezpośrednio w PowerStore lub za pośrednictwem serwerów proxy w systemie PowerMax bez zużywania zasobów hosta
- Ochrona danych Dell zapewnia przyrostową strategię tworzenia kopii zapasowych bez ograniczeń czasowych, co ogranicza ilość danych odczytywanych w pamięci masowej służącej do ochrony i przesyłanych do niej.
- PowerProtect Data Manager może zarządzać lokalnymi migawkami PowerStore (wykonywanymi co 30 minut) i tworzyć kopie zapasowe w ramach tych samych zasad w PowerProtect Data Domain (1 raz dziennie)
- Obsługa lokalnych migawek w PowerMax będzie dostępna jeszcze w tym roku
- Za pomocą jednego menedżera kopii zapasowych można chronić wiele woluminów z tego samego klastra PowerStore lub PowerMax lub z wielu klastrów

Jakie są główne elementy tej integracji?

- Rozwiązanie PowerStore komunikuje się bezpośrednio z urządzeniami PowerProtect Data Domain przez sieć LAN za pośrednictwem wbudowanego agenta i protokołu DDBoost
- Kopia zapasowa PowerMax działa na serwerze proxy
- PowerStore lub PowerMax umożliwia transfer samych zmienionych bloków, dzięki czemu między PowerStore lub PowerMax i PowerProtect Data Domain trzeba przesyłać tylko unikatowe bloki danych.
- PowerProtect Data Manager odgrywa rolę mechanizmu aranżacji między rozwiązaniami PowerStore lub PowerMax i PowerProtect Data Domain.

Jakie modele urządzeń Dell Storage są obsługiwane?

- Tylko PowerMax 4 (2500/8500)
- Wszystkie modele PowerStore T od 500T do 9200T.
- Szczegółowe informacje można znaleźć w kompletnym [przewodniku po zgodności z programem PowerProtect Data Manager](#).

Kiedy usługa Storage Direct Protection będzie dostępna z Dell Storage?

- Storage Direct Protection z PowerStore i PowerMax jest już dostępna

Jakie modele PowerProtect Data Domain są obsługiwane?

- Wszystkie modele PowerProtect Data Domain, które są obsługiwane przez program PowerProtect Data Manager
- APEX Protection Storage działające lokalnie i w chmurze publicznej (AWS)
- Szczegółowe informacje można znaleźć w kompletnym [przewodniku po zgodności z programem PowerProtect Data Manager](#).

Jakie metody ochrony są dostępne?

- Migawka lokalna PowerStore w macierzy podstawowej
- Migawka lokalna PowerStore w macierzy podstawowej i migawka zdalna w macierzy repliki
- Tworzenie kopii zapasowych na PowerProtect Data Domain za pośrednictwem macierzy podstawowej
- Tworzenie kopii zapasowych na PowerProtect Data Domain za pośrednictwem macierzy repliki
- Replikacja kopii PowerProtect Data Domain
- Retencja długoterminowa dzięki tworzeniu warstw w pamięci masowej w chmurze.
- Obsługa lokalnych migawek w PowerMax będzie dostępna jeszcze w tym roku

Jakie metody przywracania są dostępne?

- Przywracanie przyrostowe do pierwotnego lub alternatywnego woluminu PowerStore.
- PowerMax obsługuje tylko pełne przywracanie
- Przywracanie do innego lub nowego klastra w podobnym systemie (np. PowerStore do PowerStore, PowerMax do PowerMax)
- Brak obsługi przywracania między platformami (np. PowerStore do PowerMax i odwrotnie)
- Instant Access do hosta lub grupy hostów dla Power Store
- Technologia Instant Access dla PowerMax będzie dostępna w późniejszej wersji
- Przywracanie z repliki Data Domain i z kopii warstwy chmury
- Przywracanie z migawek PowerStore do oryginalnych woluminów lub klonów
- Obsługa lokalnych migawek w PowerMax będzie dostępna jeszcze w tym roku

Czy można chronić woluminy blokowe PowerStore lub PowerMax i udziały NAS?

- Tak. Program PowerProtect Data Manager obsługuje już ochronę udziałów NAS PowerStore.

- PowerMax może być chroniony jako udział rodzajowy
- Ta nowa integracja zwiększa możliwości ochrony woluminów blokowych i grup woluminów.

Jakie często używane funkcje programu PowerProtect Data Manager obsługuje ta integracja?

- Planowanie zadań zgodnie z zasadami ochrony.
- Obsługa szyfrowania podczas transferu i szyfrowania na poziomie docelowego obiektu Data Domain
- Integracja blokady przechowywania na urządzeniach DD (tryb zarządzania, tryb zgodności)
- Obsługa replikacji na urządzeniach DD.
- Obsługa tworzenia warstw DD w chmurze.
- Obsługa reguł dynamicznych dla PowerStore
 - Obsługa reguł dynamicznych dla PowerMax będzie dostępna w przyszłej wersji

Czy można współużytkować to samo urządzenie PowerProtect Data Domain z innymi obciążeniami roboczymi/aplikacjami?

- Tak, to samo urządzenie docelowe może być używane jako obiekt docelowy kopii zapasowych PowerStore lub PowerMax, a także innych obciążeń roboczych/aplikacji (opartych na Data Manager, NetWorker, Avamar lub produktach innych firm)
- Szczegółowe informacje można znaleźć w kompletnym [przewodniku po zgodności z programem PowerProtect Data Manager](#).

Więcej informacji można znaleźć w [blogu z zapowiedziami](#), w sekcji [często zadawanych pytań dotyczących rozwiązania Dell PowerStore](#), [w opisie rozwiązania PowerMax](#) oraz na stronie [Strona PowerStore 3.5 SharePoint](#)

Wykrywanie anomalii

Co to jest wykrywanie anomalii?

Wykrywanie anomalii to zaawansowana funkcja programu PowerProtect Data Manager, która zapewnia monitorowanie po zakończeniu procesu tworzenia kopii zapasowej w celu wykrycia potencjalnych zagrożeń bezpieczeństwa, takich jak ransomware. Identyfikując anomalie, dział IT ostrzega użytkowników o podejrzanych działaniach, pomagając organizacjom szybko i skutecznie reagować w celu ochrony danych.

Jak działa wykrywanie anomalii?

Wykrywanie anomalii wykorzystuje opracowane przez firmę Dell algorytmy do monitorowania kopii zapasowych w czasie rzeczywistym. Wykorzystuje trzy kluczowe metody wykrywania zagrożeń:

- **Dopasowywanie wzorców:** porównywanie metadanych plików (nazw, rozszerzeń, ścieżek) z biblioteką ponad 5000 znanych wzorców oprogramowania ransomware w celu zidentyfikowania ryzyka.
- **Analiza behawioralna:** Analizuje trendy przy użyciu uczenia maszynowego, takie jak zmiany wykorzystania danych lub nagłe szyfrowanie plików, w celu wykrycia nietypowej aktywności przy użyciu modeli szeregów czasowych.
- **Analiza konfiguracji systemu:** Skanuje ustawienia konfiguracji systemu (np. zapory ogniowe, kontrola dostępu) w poszukiwaniu luk, które ransomware mógłby wykorzystać.

Po wykryciu anomalii automatycznie wysyła alerty i zapewnia możliwość kwarantanny potencjalnie szkodliwych danych w celu dalszego zbadania. Należy pamiętać, że aby wykrywanie anomalii działało, należy włączyć wyszukiwanie i indeksowanie.

Jakie są zalety korzystania z funkcji wykrywania anomalii?

Wykrywanie anomalii zapewnia kilka kluczowych korzyści:

- **Wczesne wykrywanie zagrożeń:** Szybko identyfikuje problemy przed eskalacją, umożliwiając użytkownikom proaktywne reagowanie.
- **Lekki wpływ:** Działa bezpośrednio w środowisku produkcyjnym bez konieczności korzystania z dodatkowych zasobów infrastruktury.
- **Alerty czasu rzeczywistego:** Natychmiastowe powiadomienia o anomaliami, które umożliwiają szybsze podejmowanie decyzji.
- **Bez dodatkowych kosztów:** Pakiet PowerProtect Data Manager jest dostępny bez dodatkowych opłat.

W jaki sposób wykrywanie anomalii i CyberSense współpracują ze sobą?

Wykrywanie anomalii i CyberSense tworzą potężny duet w zakresie cyberodporności. Chociaż wykrywanie anomalii działa w środowisku produkcyjnym w celu identyfikacji zagrożeń podczas procesu tworzenia kopii zapasowej, CyberSense zapewnia dogłębną analizę śledczą izolowanych danych przechowywanych w magazynie Cyber Recovery. CyberSense wykorzystuje uczenie maszynowe oparte na sztucznej inteligencji do sprawdzania integralności danych z 99.99% precyzją i dostarcza szczegółowe raporty na temat uszkodzonych plików. Te cechy razem tworzą wielowarstwową strategię obronną. Wykrywanie anomalii zapewnia natychmiastowy wgląd, a CyberSense zapewnia inteligentne odzyskiwanie danych w przypadku cyberataku.

W jaki sposób system powiadamia użytkowników o anomaliami?

Wykrywanie anomalii wykorzystuje natywny silnik raportowania PowerProtect Data Manager do dostarczania alertów krytycznych i dodatkowych raportów. Alerty są powiązane z określonymi kopiami zapasowymi za pośrednictwem łącza „View Copy”, co umożliwia użytkownikom szybkie badanie flagowanych danych. Dodatkowe raporty, w tym dedykowana strona zdarzeń związanych z bezpieczeństwem, będą dostępne w nadchodzących aktualizacjach.

Czy istnieje dodatkowy koszt za korzystanie z funkcji wykrywania anomalii?

Nie, funkcja wykrywania anomalii jest dołączona do programu PowerProtect Data Manager bez dodatkowych kosztów. Działa natywnie w infrastrukturze lokalnej bez konieczności korzystania z narzędzi lub zasobów innych firm.

Dlaczego klienci powinni korzystać z funkcji wykrywania anomalii?

Wykrywanie anomalii dodaje proaktywną warstwę zabezpieczeń do programu PowerProtect Data Manager, wyposażając firmy w narzędzia do wczesnego identyfikowania i ograniczania ryzyka cybernetycznego. Wspiera ciągłość prowadzenia działalności biznesowej, zapewnia integralność danych i zmniejsza wpływ potencjalnych naruszeń. W połączeniu z CyberSense i niezmiennymi funkcjami PowerProtect Data Domain funkcja wykrywania anomalii pomaga tworzyć solidne, kompleksowe rozwiązanie cyberodporności dla środowisk korporacyjnych.

Archiwizacja do obiektu

Co to jest Archiwizacja do obiektu?

Archiwizacja do obiektu to nowa funkcja w programie PowerProtect Data Manager 19.19, która usprawnia długoterminowe przechowywanie danych poprzez archiwizację pełnych kopii zapasowych bezpośrednio w obiektowej pamięci masowej, takiej jak Dell ECS lub obiektowej pamięci masowej w chmurze, bez dodatkowych kosztów licencjonowania. Jest zoptymalizowany pod kątem skalowalności, elastyczności i spełnienia wymagań dotyczących zarządzania lub zgodności z przepisami.

Jakie są główne zalety funkcji Archive to Object?

- **Wydajna archiwizacja:** Zautomatyzowane przepływy pracy oparte na regułach ograniczają ręczne nakłady pracy na potrzeby długoterminowego przechowywania.
- **Elastyczne przywracania:** Umożliwia bezpośrednie przywracanie z pamięci masowej obiektów bez konieczności przechodzenia przez Data Domain, co pozwala zaoszczędzić czas i uprościć procesy.
- **Skalowalna pamięć masowa:** Obsługuje znaczne obciążenia robocze dzięki archiwizacji do 200 TB dziennie i 1 PB tygodniowo.
- **Opłacalność:** Usługa dostępna bez dodatkowych opłat dla użytkowników PowerProtect Data Manager (płać tylko za pamięć masową ECS).

Jak działa archiwizacja do obiektu?

- Archiwizacja pełnych kopii zapasowych z PowerProtect Data Domain do obiektowej pamięci masowej za pośrednictwem silnika ochrony.
- Metadane są przechowywane w repozytorium obiektów w celu obsługi bezproblemowego odzyskiwania danych.
- Przywracanie może odbywać się bezpośrednio do miejsca docelowego odzyskiwania, co eliminuje zależność od Data Domain przy odzyskiwaniu.

Jakie są główne zastosowania archiwizacji do obiektu?

- **Zarządzanie i zgodność z przepisami:** Upraszcza retencję długoterminową w celu spełnienia wymogów regulacyjnych.
- **Cyberodporność:** zabezpieczanie dodatkowych kopii zapasowych w obiektowej pamięci masowej w celu zwiększenia możliwości odzyskiwania.
- **Skalowalna archiwizacja:** Wydajna obsługa potrzeb archiwizacji danych na dużą skalę.

Jakie obciążenia robocze są obsługiwane przez funkcję Archiwizacja do obiektu?

Wstępna pomoc techniczna obejmuje:

- Kopie zapasowe VMWare (przezroczyste zrzuty i kopie zapasowe oparte na VADP).
- Kopie zapasowe systemu plików (FBB) dla systemów Linux i Windows.

Planowane wsparcie przyrostowych kopii zapasowych, dodatkowych systemów plików i obciążeń roboczych, takich jak kopie zapasowe baz danych, będzie następowało w kolejnych wersjach.

Jak Archiwizacja do obiektu wypada w porównaniu z funkcją Warstwa chmury?

- **Elastyczność:** archiwizacja do obiektu umożliwia bezpośrednie przywracanie do miejsc docelowych odzyskiwania, podczas gdy warstwa chmury wymaga przywrócenia najpierw do Data Domain.
- **Limity dzienne/tygodniowe:** Archiwizacja do obiektu obsługuje większą przepustowość (200 TB/dzień, 1 PB/tydzień) w porównaniu z warstwą chmury.
- **Kompresja:** Archiwizacja do obiektu kompresuje dane, ale nie deduplikuje się tak jak Warstwa chmury.
- **Kopia zapasowa:** archiwizacja do obiektu tworzy drugą kopię, poprawiając cyberodporność, gdy warstwa chmury przenosi dane.

Czy istnieją jakieś ograniczenia dotyczące archiwizacji do obiektu?

- Obecnie obsługuje tylko maszyny wirtualne VMWare i systemy plików. Dodatkowe przypadki użycia zostaną rozszerzone w nadchodzących wersjach.
- Wstępna pomoc techniczna jest ograniczona do Dell ECS. Usługi AWS, Google Cloud i Azure zostaną dodane później.
- Obsługiwane są pełne kopie zapasowe. Dla wersji 19.20 planowane są przyrostowe kopie zapasowe.
- Brak indeksu zarchiwizowanej zawartości, wymagającego pełnego odzyskiwania kopii zapasowej w celu przywrócenia określonego pliku.
- W ramach przyszłych aktualizacji planowane jest przywracanie pamięci podręcznej i indeksowane.

Raportowanie wielu systemów

Co to jest raportowanie wielu systemów?

Raportowanie wielu systemów to nowa funkcja w programie PowerProtect Data Manager 19.19, która zapewnia scentralizowane monitorowanie i raportowanie do 150 systemów. Łączy krytyczne punkty danych, takie jak zadania, kopie, alerty i kondycja systemu, w jeden, intuicyjny interfejs, zmniejszając złożoność i poprawiając wydajność operacyjną.

Jakie są najważniejsze funkcje raportowania wielu systemów?

- **Scentralizowane monitorowanie:** Zarządzanie maksymalnie 150 instancjami PowerProtect Data Manager lub urządzeniami PowerProtect Data Manager z jednej konsoli.
- **Kompleksowe raportowanie:** Uzyskaj wgląd w zadania, pamięć masową, alerty, dzienniki inspekcji, kondycję systemu i nie tylko.

- **Konfigurowalne pulpity nawigacyjne:** Zacznij od gotowych szablonów lub twórz dostosowane pulpity nawigacyjne dostosowane do Twoich potrzeb.
- **Zaawansowane narzędzia raportowania:** Wykorzystaj funkcje korporacyjne Grafana, takie jak harmonogramowanie, logowanie jednokrotne (SSO) i wsparcie wielomiejscowości.
- **Przechowywanie danych:** Zachowaj dane historyczne do 18 miesięcy dzięki automatycznemu zarządzaniu przechowywaniem w celu uzyskania pełnej widoczności.
- **Projekt Future-Proof:** Stworzony z myślą o integracji dodatkowych produktów w ramach tej samej struktury monitorowania i raportowania.

W jaki sposób raportowanie wielu systemów poprawia wydajność klientów?

Raportowanie wielu systemów upraszcza zarządzanie, konsolidując informacje z wielu systemów w jednym interfejsie. Administratorzy IT mogą skrócić czas poświęcany na przechodzenie między różnymi systemami, aby bardziej skupić się na użytecznych danych w celu podejmowania lepszych i szybszych decyzji. Dzięki zaawansowanym funkcjom, takim jak konfigurowalne pulpity nawigacyjne i narzędzia Grafana, użytkownicy mogą dostosować swoje środowisko do określonych potrzeb biznesowych, co jeszcze bardziej zwiększa wydajność.

Czy pulpity nawigacyjne i raporty w raportach wielosystemowych można dostosować?

Tak. Raportowanie wielu systemów zawiera wstępnie zaprojektowane szablony pulpitu nawigacyjnego, które ułatwiają szybkie rozpoczęcie pracy. Użytkownicy mogą również dostosować istniejące pulpity nawigacyjne lub tworzyć zupełnie nowe pulpity zgodnie z określonymi wymaganiami operacyjnymi. Ponadto użytkownicy mogą bezpośrednio uzyskać dostęp do bazy danych w celu zapytań ad hoc i integracji z narzędziami specyficznymi dla klienta.

W jaki sposób raportowanie wielu systemów obsługuje dane historyczne?

Raportowanie wielu systemów domyślnie przechowuje dane historyczne przez okres do 18 miesięcy, a automatyczne zarządzanie przechowywaniem pozwala zachować aktualność i porządek informacji bez dodatkowego wysiłku.

Jakie są przyszłe plany rozwoju raportowania wielosystemowego?

Przyszłe aktualizacje mają na celu rozszerzenie możliwości raportowania wielu systemów, w tym głębszą integrację z dodatkowymi produktami Dell do ochrony danych oraz ulepszone funkcje proaktywnego zarządzania i zaawansowanej analizy.

Oparta na chmurze analityka i monitorowanie

Co to jest PowerProtect Central?

Od kwietnia 2021 r. rozwiązanie Dell APEX AIOps (dawniej CloudIQ) zastąpi usługę PowerProtect Central, umożliwiając monitorowanie i analizę w chmurze dla programu PowerProtect Data Manager. Użytkownicy usługi PowerProtect Central zostaną przekierowani do Dell APEX AIOps.

Co to jest Dell APEX AIOPS i jakie możliwości zapewnia klientom korzystającym z programu PowerProtect Data Manager?

Dell APEX AIOPS (dawniej CloudIQ) zapewnia telemetrię, uczenie maszynowe i analizę predykcyjną w celu proaktywnego podejmowania działań i szybszego rozwiązywania problemów. W przypadku każdego wystąpienia programu PowerProtect Data Manager rozwiązanie Dell APEX AIOPS zapewnia następujące możliwości:

- podsumowanie informacji o ochronie danych,
- raport dotyczący ochrony zasobów,
- szczegółowe informacje o ochronie zasobów,
- raporty dotyczące zgodności zasobów z przepisami,
- szczegóły konfiguracji,
- Alerty

Więcej szczegółów można znaleźć w [Centrum wiedzy na temat rozwiązania Dell APEX AIOPS-PowerProtect](#) oraz [na stronie internetowej Dell APEX AIOPS](#).

Ochrona obciążeń roboczych w chmurze oparta na modelu SaaS

Co to jest Cloud Snapshot Manager?

PowerProtect Cloud Snapshot Manager to rozwiązanie SaaS, które ułatwia ochronę krytycznych obciążeń roboczych w chmurze publicznej poprzez wykorzystanie podstawowej technologii migawek dostawców chmury bez konieczności instalacji lub posiadania infrastruktury. Klienci mogą wykrywać, aranżować i automatyzować ochronę obciążeń roboczych na platformach AWS i Azure za pomocą zasad opartych na znacznikach. Klienci mogą aktywować aplikację Cloud Snapshot Manager przy użyciu licencji na rozwiązanie PowerProtect Data Manager.

Jakie możliwości są dostępne w ramach integracji aplikacji Cloud Snapshot Manager z programem PowerProtect Data Manager?

Alerty programu PowerProtect Data Manager uwzględniają zdarzenia aplikacji Cloud Snapshot Manager, w tym podsumowanie alertów. W programie Data Manager można skonfigurować aplikację Cloud Snapshot Manager jako źródło zasobów, a na pulpicie nawigacyjnym dostępne jest szczegółowe podsumowanie, w tym łączna liczba chronionych i niechronionych zasobów, liczba zadań, które zakończyły się powodzeniem lub niepowodzeniem itp. Użytkownicy mogą połączyć się z aplikacją Cloud Snapshot Manager i uruchomić ją, aby uzyskać więcej informacji i zarządzać zadaniami.

Na czym polega korzyść dla klientów korzystających z aplikacji Cloud Snapshot Manager?

Wraz z rozwojem infrastruktury w chmurze publicznej przedsiębiorstwa stają przed nowymi wyzwaniami związanymi z ochroną obciążeń roboczych w chmurze. Nieodłączne korzyści płynące z chmury, takie jak elastyczność zasobów, łatwość tworzenia wystąpień nowych maszyn wirtualnych i nowych baz danych PaaS w oparciu o interfejs API, są bardzo cenne, ponieważ umożliwiają pełne wykorzystanie potencjału

IT na żądanie. Potrzebne jest jednak rozwiązanie, które nie wymaga agentów i udostępnia rozbudowane interfejsy API do automatyzacji. Firmy muszą także chronić wiele nowych źródeł danych — zarówno tradycyjne aplikacje działające w infrastrukturze chmury, jak i nowe aplikacje chmurowe, które korzystają z usług PaaS (DBaaS, K8aaS, usługi plików). W celu osiągnięcia pełnej automatyzacji chmury niezbędny jest rozbudowany zestaw interfejsów API. Wymagana jest także kontrola nad wieloma oddzielnymi kontami w chmurze bez konieczności tworzenia nowej infrastruktury dla każdego konta lub kumulowania kosztów transferu danych między chmurami VPC / kontami. Aplikacja Cloud Snapshot Manager zapewnia takie możliwości.

Narzędzie Cloud Snapshot Manager można aktywować za pomocą licencji na rozwiązanie PowerProtect Data Manager, więc klienci nie muszą wybierać między tymi produktami ani kupować ich osobno. Otrzymują oba te rozwiązania w pakiecie. Dzięki temu mogą chronić swoje aplikacje firmowe dzięki zaawansowanym funkcjom rozwiązań PowerProtect Data Manager i APEX Protection Storage, a jednocześnie obsługiwać tysiące maszyn wirtualnych i innych baz danych PaaS za pomocą opartych na znacznikach funkcji ochrony w aplikacji Cloud Snapshot Manager bez konieczności instalowania jakichkolwiek agentów lub infrastruktury w chmurze.

Gdzie można dowiedzieć się więcej o aplikacji Cloud Snapshot Manger?

Wszystkie przydatne zasoby na temat sprzedaży i produktu są dostępne na [stronie SharePoint dotyczącej aplikacji PowerProtect Data Manager](#).

PowerProtect Cyber Recovery

Co to jest PowerProtect Cyber Recovery?

Rozwiązanie PowerProtect Cyber Recovery automatyzuje tworzenie i ochronę pierwowzorów w odizolowanym magazynie danych, umożliwiając niezawodne przepływy pracy analizy danych w środowisku typu „clean room”.

Narzędzie tworzy niezmienną kopię metadanych modułu przenoszenia danych PowerProtect Data Manager (np. katalogu kopii zapasowych) w odizolowanym środowisku i pozwala odzyskiwać zapisane zestawy PowerProtect Data Manager z powrotem do środowiska produkcyjnego lub do tymczasowego odizolowanego środowiska odzyskiwania.

Rozwiązanie PowerProtect Cyber Recovery pozwala wdrożyć zautomatyzowany przepływ pracy w celu rozszerzenia infrastruktury ochrony danych o rzeczywistą izolację danych, analizę danych śledczych, analizę i — co najważniejsze — odzyskiwanie danych zwiększające odporność na awarie.

Czy rozwiązanie PowerProtect Cyber Recovery jest licencjonowane oddzielnie od programu PowerProtect Data Manager?

Chociaż narzędzie Cyber Recovery należy włączyć za pomocą oddzielnego klucza licencyjnego, ta licencja jest bezpłatna i można ją uzyskać w ramach procesu zamawiania programu PowerProtect Data Manager.

Licencja na PowerProtect Cyber Recovery jest częścią uprawnień dostępnych po zakupie programu PowerProtect Data Manager.

Czy rozwiązanie PowerProtect Cyber Recovery jest dostępne z poziomu programu PowerProtect Data Manager?

Nie. Rozwiązanie PowerProtect Cyber Recovery z założenia jest zarządzane i kontrolowane z poziomu serwera Cyber Recovery Vault Management Server. W interfejsie zarządzania programem PowerProtect Data Manager nie pojawiają się żadne informacje o wystąpieniu Cyber Recovery.

Gdzie można dowiedzieć się więcej o rozwiązaniu PowerProtect Cyber Recovery?

Wszystkie przydatne zasoby na temat sprzedaży i produktu są dostępne na [stronie SharePoint dotyczącej aplikacji PowerProtect Cyber Recovery](#).

Path to PowerProtect

Co to jest Path to PowerProtect?

Path to PowerProtect to narzędzie dla klientów, które pomaga im w przejściu z rozwiązania Avamar na program PowerProtect Data Manager. Obecnie głównym celem narzędzia jest pomoc we wdrażaniu zasad ochrony danych rozwiązania Data Manager przez wykorzystanie istniejących zasad Avamar.

Jakie obciążenia robocze są obecnie obsługiwane przez narzędzie Path to PowerProtect?

Narzędzie Path to PowerProtect obsługuje migrację zasad dotyczących rozwiązań VMware, systemów plików (w tym Windows i Linux), SQL i Oracle. Narzędzie będzie obsługiwać tworzenie nowych zasad programu PowerProtect Data Manager w oparciu o istniejące zasady Avamar LUB przypisywanie zasobów w ramach zasady Avamar do istniejących zasad Data Manager.

Jakie obciążenia robocze są planowane?

Zgodnie z planem narzędzie Path to PowerProtect będzie obsługiwać system AIX w tym roku i NDPM w przyszłości.

Czy narzędzie Path to PowerProtect obsługuje obecnie urządzenie PowerProtect Data Manager Appliance (DM5500)?

Wsparcie dla DM5500 będzie oficjalnie dostępne w następnej wersji, 1.0.6, która ma zostać udostępniona 19.06.2023. Klienci, którzy potrzebują obsługi urządzenia DM5500 jako obiektu docelowego migracji, mogą przesłać prośbę o wycenę.

Czy narzędzie Path to PowerProtect jest dostępne dla klientów?

Narzędzie Path to PowerProtect jest obecnie dostępne za pośrednictwem działu ds. usług w przypadku klientów korzystających z oprogramowania Data Manager.

Jaki jest koszt narzędzia?

Narzędzie jest dostępne dla klientów bezpłatnie w ramach uprawnień objętych licencją na oprogramowanie PowerProtect Data Manager.

Jak uzyskać dostęp do narzędzia Path to PowerProtect?

Narzędzie jest autonomiczną aplikacją OVA, którą można uzyskać od działu ds. usług. Dział ds. usług może udostępnić narzędzie do pobrania i pomóc w jego instalacji. Po zakończeniu migracji zespół ds. usług może również pomóc w odinstalowaniu narzędzia.

Czy narzędzie będzie dostępne bezpośrednio dla klientów?

Tak, planujemy wprowadzenie wersji ogólnodostępnej, której klienci będą mogli używać po zainstalowaniu. WSZYSCY klienci korzystający z rozwiązania Data Manager będą uprawnieni do korzystania z tego narzędzia.

Dlaczego Path to PowerProtect to oddzielne narzędzie, które nie jest zintegrowane z programem PowerProtect Data Manager?

Path to PowerProtect jest obecnie oddzielnym narzędziem, dzięki czemu możemy reagować na wymagania klientów i stopniowo wprowadzać nowe funkcje. Narzędzie ma na celu pomoc w migracji, a dzięki oddzieleniu go od programu Data Manager jesteśmy w stanie szybciej dodawać aktualizacje bez konieczności wprowadzania zmian w rozwiązaniu Data Manager. Plan zakłada połączenie narzędzia z programem Data Manager jako wbudowanego rozwiązania migracji po zapewnieniu obsługi podstawowych obciążeń roboczych i spełnieniu większości próśb klientów dotyczących funkcji.

Co z migracją danych i umożliwieniem klientom wycofania systemów Avamar?

Zamierzamy umożliwić klientom wycofywanie systemów Avamar. W tym celu konieczne będzie przeniesienie bieżącego katalogu kopii do innego systemu Avamar. Zapewnimy klientom możliwość migracji obecnych systemów Avamar do jednego wystąpienia AVE, które będzie zarządzać ich kopiami do LTR na urządzeniach PowerProtect Data Domain. Kopie będą dostępne do celów sprawozdawczości w zakresie odzyskiwania i audytów.

Kiedy narzędzie Path to PowerProtect umożliwi klientom wycofywanie systemów Avamar?

Wprowadzenie możliwości konsolidacji systemów Avamar klienta w celu obsługi ich wycofywania jest planowane na koniec roku kalendarzowego 2023.

Gdzie można znaleźć więcej informacji na temat narzędzia Path to PowerProtect?

Poniżej znajdują się łącza do różnych wersji demonstracyjnych, warsztatów, podręczników administratora i informacji dotyczących wydania przedstawiających podstawowe funkcje narzędzia:

Interaktywne prezentacje:

- [Path to PowerProtect — migracja zasad dotyczących maszyn wirtualnych](#)
- [Path to PowerProtect — migracja zasad dotyczących baz danych SQL](#)

Warsztaty:

- Ścieżka do przewodnika PowerProtect – [HOL0419-02](#)

Wewnętrzne prezentacje techniczne:

- [Podręcznik administratora](#)
- [Informacje dotyczące wydania](#)
- [Podręcznik wdrażania](#)

Informacje dotyczące wydania:

- [Informacje dotyczące wydania narzędzia Dell Path to PowerProtect](#)

Nowoczesna architektura oparta na usługach

Jakie korzyści zapewnia klientom nowoczesna architektura oparta na usługach?

Wraz z transformacją środowiska klienta program PowerProtect Data Manager umożliwia szybką ewolucję w celu spełnienia przyszłych wymagań IT dzięki interfejsom API pozwalającym na skalowanie usług.

Dążymy do częstszego wprowadzania nowych wersji produktów PowerProtect, aby zapewnić ciągłe innowacje przy minimalnym wpływie na proces uaktualniania.

Zasoby z zakresu wspierania sprzedaży

Licencjonowanie

Jestem pracownikiem firmy Dell i potrzebuję licencji do celów testowych. Jak mogę ją uzyskać?

Możesz utworzyć zgłoszenie serwisowe z prośbą o licencję NFR. Po otrzymaniu formularza NFR należy go wypełnić i postępować zgodnie z zawartymi w nim instrukcjami.

W jaki sposób jest licencjonowany program PowerProtect Data Manager?

PowerProtect Data Manager jest licencjonowany na podstawie ilości danych frontonu (Front End Terabyte — FETB) i na podstawie liczby procesorów, zarówno w ramach licencji bezterminowej, jak i subskrypcji. Więcej informacji można znaleźć w następujących przewodnikach po zamawianiu i licencjonowaniu oprogramowania do ochrony danych:

[Przewodnik po licencjonowaniu](#)

Czy klient może zsumować pojemność, która ma być chroniona w wielu lokalizacjach, aby zakwalifikować się do określonego poziomu pojemności?

Tak. Nie ma ograniczeń co do liczby lokalizacji, w których można wdrożyć program PowerProtect Data Manager.

Zamawianie i pomoc techniczna

Jak zamówić program PowerProtect Data Manager?

Wszystkie wersje programu PowerProtect Data Manager można zamówić w systemie DSA/Gii.

Jakie są limity pojemności lub liczby procesorów w przypadku wersji PowerProtect Data Manager Essentials?

W przypadku wersji PowerProtect Data Manager Essentials obowiązuje limit 50 TB lub procesorów.

Jakiego rodzaju usługi pomocy technicznej są dostępne dla programu PowerProtect Data Manager i kiedy należy je rekomendować?

Pakiet ProSupport Infrastructure Suite pozwala rozwiązywać problemy IT w krótszym czasie i przy mniejszym wysiłku ze strony klienta, często umożliwiając wykrywanie problemów jeszcze przed ich wystąpieniem. Rekomendacje usług pomocy technicznej często zależą od złożoności środowiska klienta i sposobu alokacji zasobów IT. Dostępne opcje obejmują:

- **ProSupport Plus:** gdy polecisz nasz najwyższy poziom wsparcia, klienci uzyskają wszystkie funkcje usługi ProSupport i wyższy poziomu personalizacji, w tym dostęp do wyznaczonego przedstawiciela handlowego ds. usług, priorytetowy dostęp do ekspertów ds. pomocy technicznej, a także dostęp do analizy predykcyjnej umożliwiającej zapobieganie problemom dzięki naszej Bramce zabezpieczeń. Pakiet ProSupport Plus z usługą Mission Critical obejmuje 4-godzinny czas reakcji w przypadku wymiany części na miejscu w zależności od poziomu istotności problemu.
- **ProSupport:** eksperci rozwiązują problemy IT 7 dni w tygodniu, 24 godziny na dobę. Nasi wykwalifikowani specjaliści rozwiązują problemy związane ze sprzętem i oprogramowaniem systemów w centrum przetwarzania danych. Pakiet można zakupić z opcją serwisu w następnym dniu roboczym LUB z 4-godzinnym czasem reakcji w ramach usługi Mission Critical.

Pakiet ProDeploy Infrastructure Suite zapewnia klientom największe korzyści z technologii już od pierwszego dnia po wdrożeniu. Z programem PowerProtect Data Manager dostępne są następujące opcje pakietu ProDeploy Infrastructure Suite:

- **ProDeploy Plus:** najlepszy wybór w przypadku optymalizacji długoterminowej wydajności systemów o znaczeniu krytycznym z pojedynczym punktem kontaktu do zarządzania projektami w regionie. Usługa ProDeploy Plus obejmuje całodobową instalację i konfigurację oprogramowania systemowego na miejscu, 30-dniową pomoc w konfiguracji po wdrożeniu oraz punkty szkoleniowe w ramach usług Dell Education Services.
- **ProDeploy:** specjalistyczne planowanie, instalacja i konfiguracja, aby pomóc klientom w szybkim wdrożeniu nowych technologii, z pojedynczym punktem kontaktu do zarządzania projektami. Usługa ProDeploy obejmuje planowanie wdrożenia, całodobową instalację sprzętu na miejscu oraz całodobową instalację i konfigurację oprogramowania systemowego, a także dokumentację projektową i przekazywanie wiedzy.
- **Production Ready for Backup:** po wdrożeniu rozwiązania Data Manager usługa Production Ready for Backup obejmuje personalizację tej technologii, analizę konkretnego środowiska klienta oraz przełożenie jego potrzeb na zasady dotyczące tworzenia kopii zapasowych i ochrony danych. Usługa jest zalecana w przypadku klientów z wymaganiami prawnymi, konkretnymi wyzwaniami związanymi z umowami SLA lub lukami w kompetencjach w zakresie ochrony danych. Usługę można zakupić z usługą ProDeploy / ProDeploy Plus lub samodzielnie.

- **Dodatkowe usługi wdrożeniowe:** firma Dell oferuje specjalistyczne usługi umożliwiające zwiększenie skali lub możliwości poza standardowy zakres usług ProDeploy, ProDeploy Plus i Production Ready. Te dodatki służą do wdrażania określonych opcjonalnych funkcji rozwiązania Data Manager bez płacenia za usługi, których klient nie potrzebuje — wszystkie dodatkowe elementy można łatwo zamówić jako oddzielne numery SKU. Są dostępne w punkcie sprzedaży lub później.
- **Dodatkowy czas wdrożenia:** standardowa usługa z elastycznym zakresem obejmująca 4-godzinne bloki zdalne lub 8-godzinne bloki na miejscu, świadczona przez certyfikowanego eksperta z firmy Dell. Służy do uzupełnienia pakietu ProDeploy Infrastructure Suite o dodatkowe lub nieobjęte zakresem opcje — od razu lub w ciągu 1 roku po zakupie. Usprawnia realizację i minimalizuje potrzebę niestandardowych SOW.

Dodatkowy czas wdrożenia można wykorzystać na różne zadania, takie jak:

- Rozszerzony zakres: dodatkowe wymagania wykraczające poza oferty standardowe.
- Nieprzewidziane potrzeby: pomoc w nieoczekiwanych przypadkach w ciągu pierwszego roku.
- Zadania ad hoc: potrzeby krótkoterminowe bez wysiłku związanego z niestandardowym procesem wyceny.
- **Usługi migracji danych:** pomagają w efektywnym przenoszeniu danych, ułatwiając przejście na nowe produkty firmy Dell do ochrony danych oraz odciążając dział IT i administratorów. Idealne rozwiązanie dla klientów, którzy wdrażają nowe technologie pamięci masowej, konsolidują rozproszone dane lub mają obawy bądź problemy związane z terminowym przeprowadzeniem migracji w ramach większej inicjatywy.
- **Usługi świadczone na miejscu:** idealne rozwiązanie dla klientów korzystających z rozwiązania PowerProtect w ramach dużej bazy instalacyjnej lub złożonych środowisk. Usługi świadczone na miejscu obejmują wyznaczonego eksperta ds. ochrony danych, który uzupełnia braki w zasobach, zarządza codziennymi operacjami i pomaga zespołom przejść na nowe technologie. Dostępne w minimalnych okresach 1 i 2 tygodni.

Jak zamówić usługi profesjonalne lub usługi edukacyjne dla klientów?

Najpopularniejsze usługi profesjonalne są dostępne w narzędziach do zamawiania firmy Dell. Usługi, które nie zostały wymienione, należy zamówić w ramach poszczególnych ścieżek rozwiązań technologicznych.

Jak zamówić usługi standardowe w punkcie sprzedaży?

W przypadku sprzedaży nowego sprzętu i oprogramowania Data Manager usługi są dostępne w narzędziach do zamawiania firmy Dell.