Marzo 2025

Domande frequenti: PowerProtect Data Manager

Sommario

Domande frequenti: PowerProtect Data Manager **1**

Panoramica **2**

Novità di PowerProtect Data Manager 19.19 (marzo 2025) 3

Novità di PowerProtect Data Manager 19.18 (novembre 2024) 3

Novità di PowerProtect Data Manager 19.17 (luglio 2024) 4

Novità di PowerProtect Data Manager 19.16 (marzo 2024) 5

Novità di PowerProtect Data Manager 19.15 (novembre 2023) 6

Novità di PowerProtect Data Manager 19.14 (luglio 2023) 7

Novità di PowerProtect Data Manager 19.13 (marzo 2023) 8

Novità di PowerProtect Data Manager 19.12 (ottobre 2022) 8

Novità di PowerProtect Data Manager 19.11 (giugno 2022) 9

Novità di PowerProtect Data Manager 19.10 (marzo 2022) 10

Novità di PowerProtect Data Manager 19.9 (settembre 2021) 11

Introduzione di PowerProtect Data Manager Essentials (giugno 2021) 13

Novità di PowerProtect Data Manager 19.8 (maggio 2021) 13

Novità di PowerProtect Data Manager 19.7 (febbraio 2021) 15

Novità di PowerProtect Data Manager 19.6 (ottobre 2020) 15

Novità di PowerProtect Data Manager 19.5 16

Che cos'è PowerProtect Data Manager? 17

Funzionalità di PowerProtect Data Manager 19

PowerProtect Data Manager 20

Ottimizzazione multicloud 22

Application Direct 23

File System Agent 24

Plug-in DDBoost File System (BoostFS) 24

Supporto di VMware e virtualizzazione 25

Supporto di hypervisor Hyper-V 28

Protezione Storage Direct 29

Protezione Storage Direct con Dell Storage 30
Rilevamento di anomalie 32
Archiviazione a oggetti 34
Reporting multi-sistema 35
Monitoraggio e analisi basati sul cloud 36
Protezione basata su SaaS di carichi di lavoro nel cloud 37
PowerProtect Cyber Recovery 38
Path to PowerProtect 38
Architettura moderna basata su servizi 40
Supporto alle vendite 40
Licenze 40
Ordinazione e assistenza 41

Panoramica

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

Novità di PowerProtect Data Manager 19.19 (marzo 2025)

Miglioramenti dei carichi di lavoro

- Estensione del supporto dell'ecosistema: hypervisor Hyper-V, Azure Local, virtualizzazione OpenShift, PostreSQL
- Transparent Snapshot: supporto di Google Cloud VMware Engine (GCVE)
- File system: ripristino reindirizzato alla cartella New/Alternative, indicizzazione del file system XFS per i backup BBB
- NAS: supporto di PowerScale/Isilon Change File List, supporto di NetApp Multi-Node HA

Sicurezza aggiornata

- Rilevamento delle anomalie (GA)
- Autenticazione a più fattori (MFA): Google e Microsoft Authenticator

Interfaccia utente migliorata

- Reporting multi-sistema
- Archiviazione a oggetti per le macchine virtuali e i file system - solo ECS
- Data Manager, protezione VMware-HA
- Supporto dell'opzione di aggiornamento del proxy manuale per i clienti
- Supporto del sistema operativo localizzato - portoghese (Brasile)

Storage Element Protection

- Supporto per il ripristino rapido
- Strumento CLI di backup e ripristino
- PowerMax
  - Creazione automatica di gruppi di storage di ripristino
  - Mappatura di volumi di ripristino/gruppi di storage

Per ulteriori informazioni, leggere la presentazione Novità di PowerProtect Data Manager 19.19.

Novità di PowerProtect Data Manager 19.18 (novembre 2024)

Dell Storage

- PowerMax
  - Gestione snapshot locali con protezione Storage Direct
  - MEDITECH, supporto Server DR
  - Prestazioni migliorate (operazioni bitmap snapshot, ripristino blocchi usati)
  - Strumento di ripristino di emergenza autonomo
- PowerMax e PowerStore
  - Attivazione/disattivazione della crittografia DDBoost
  - Raccolta delle dimensioni su licenza

- Supporto al riavvio del processo di protezione

Sicurezza aggiornata

- Rilevamento delle anomalie (anteprima tecnologica)
- Scadenza Configurable Root Certificate

Miglioramenti dei carichi di lavoro

- NAS – Supporto MultiVLAN, integrazione snapshot a singolo nodo con NetApp.
- Visualizzazione della copie Avamar nell'UI di PowerProtect Data Manager
- Opzione di installazione automatica per Transparent Snapshots VIB
- Backup parallelo migliorato per PowerProtect Data Domain HA con TSDM

Aggiornamenti del database

- Parallelismo a livello host SQL lato client per i backup
- Ripristino granulare di Active Directory utilizzando le appartenenze ai gruppi utenti

Interfaccia utente migliorata

- Copie: funzionalità di ricerca tag DIA (Data Invulnerability Architecture)
- Supporto del sistema operativo localizzato - portoghese (Brasile)
- Supporto PowerMax 10.2.0, DDOS 8.1, AlmaLinux

Per ulteriori informazioni, leggere la presentazione Novità di PowerProtect Data Manager 19.18.

Novità di PowerProtect Data Manager 19.17 (luglio 2024)

Carichi di lavoro supportati

- Integrazione della Protezione PowerMax Storage Direct
- Protezione PowerStore Storage Direct con backup coerenti con le applicazioni
- Supporto Oracle Exadata e agente Windows per Oracle RMAN
- Selezione della compressione ottimizzata per le app
- Backup multi-streaming di file e backup basati su blocchi per Linux
- Ripristino rapido Restore AppAware SQL su supporto alternativo
- Supporto File System Agent per Debian Linux 9 e 10

Sicurezza aggiornata

- Rilevamento delle anomalie (beta)
- Prompt/accesso VMware 2FA con ripristino a livello di file
- Generazione di registri di audit per le prossime scadenze dei certificati di terze parti
- Supporto per la firma CA intermedia
- Avvisi per log mancanti

Miglioramenti per NAS

- Supporto del backup di file e condivisioni NAS con autorizzazioni 700, 500, 400
- Abilitazione del reindirizzamento dei restore dei file NAS all'interno della stessa share
- Opzione per evitare la sovrascrittura durante le operazioni di restore NAS
- Supporto per il ripristino rapido

Interfaccia utente migliorata

- Miglioramento del tracciamento dell'utilizzo di FETB per gli asset e le policy di protezione (VM, agenti, K8)
- RBAC per pre/post script
- Gestione degli hotfix tramite interfacce utente
- Supporto per sistemi operativi localizzati: cinese tradizionale e spagnolo

Per ulteriori informazioni, leggere la presentazione Novità di PowerProtect Data Manager 19.17.

Novità di PowerProtect Data Manager 19.16 (marzo 2024)

Interfaccia utente migliorata

- Filtri dei file: aggiunta di elementi da includere, ulteriori filtri e interfaccia utente reinventati per backup basati su file e NAS
- Script precedenti e successivi per le policy di protezione dell'agent delle applicazioni
- Gestione delle copie dei cataloghi, incluse le operazioni di ricerca, eliminazione e mantenimento degli aggiornamenti delle copie
- Procedura guidata per le attività di protezione
- Backup self-service con diritti non amministrativi per SQL, Oracle RMAN, file system, SAP HANA in esecuzione su piattaforma Unix.
- Miglioramenti della generazione di log
- DDOS 8.0 in esecuzione su hardware 16G
- Supporto di vSphere 8.0 U2
- Transparent Snapshots e supporto VADP per VMS su vSAN ESA
- Lettura più rapida di file di piccole dimensioni su FNSv3
- Supporto di NAS FS 4.1/4.2

Carichi di lavoro supportati

- Elenco dei fornitori certificati SAP per SAP HANA
- Ripristino rapido per SQL App Direct, SAP HANA, Exchange, Oracle e VMware FLR
- Restore delle VM eliminate con l'UUID originale
- Supporto di Oracle Exadata (anteprima tecnica)
- Oracle: prestazioni di backup migliorate per la compressione e il database abilitato per TDE

- Exchange: ripristino multi-database
- Supporto per il restore di Distributed Resource Scheduler (DRS)
- Riavvio dei processi in esecuzione dopo l'aggiornamento
- Indice dei file system ZFS

Per ulteriori informazioni, leggere la presentazione Novità di PowerProtect Data Manager 19.16.

Novità di PowerProtect Data Manager 19.15 (novembre 2023)

Supporto esteso per i carichi di lavoro

- Restore centralizzato di SAP HANA
- Restore centralizzato di Exchange
- Oracle RAC: backup multi-stream e modalità passiva attiva
- Hadoop Standalone Agent
- MetaCache Database (MCDB) su Exchange 2019
- Ottimizzazione degli slicer per file system NAS ad alta densità con protezione dei NAS dinamica
- Backup di Protezione Storage Direct basati su blocchi direttamente in APEX Protection Storage

Miglioramenti del file system

- Ripristino a livello granulare di Active Directory
- Coesistenza per l'agent File System Agent (FSA) con gli agent DDBEA e Data Manager
- Selezione di backup basato su blocchi o su file
- Supporto per Rocky Linux 8 e 9
- Supporto della ZFS

Sicurezza aggiornata

- Crittografia dei metadati e dei registri di sistema
- Manage File Replication (MFR) seleziona automaticamente l'opzione più sicura disponibile
- Convalida rigorosa per le API REST pubbliche
- Possibilità di rimuovere Retention Lock Governance (RLG) dalla copia di backup selezionata
- Replication Lock Compliance (RLC) e integrazione dell'engine di reporting per PowerStore

Esperienza del cliente di livello superiore

- Supporto in lingua coreana per i nomi degli asset e dell’origine degli asset
- Policy di protezione dei clone
- Riattivazione automatica dei processi dopo l'aggiornamento per NAS e agent applicativi
- Rilevamento delle copie create dopo un evento DR
- Indicazione di come sono stati originati i processi (pianificati, manuali)

- Delta dei job di protezione tra il job più recente e quello precedente (numero di asset, dimensione del backup, durata)

Per ulteriori informazioni, leggere la presentazione Novità di PowerProtect Data Manager 19.15.

Novità di PowerProtect Data Manager 19.14 (luglio 2023)

Supporto appliance

- Supporto per array di storage PowerStore
  - Backup e ripristino incrementali perenni dei volumi PowerStore su PowerProtect Data Domain/APEX Protection Storage e DM5500
  - Gestione delle istantanee PowerStore locali con Data Manager
  - Backup e ripristino coerenti con l'arresto anomalo con gestione centralizzata
  - Supporto per l'accesso istantaneo da copie DD
  - Ripristino all'array PowerStore originale e alternativo da primario/copia di replica
- Qualifica di Oracle Database Appliance (ODA)

Miglioramenti di VMware e container

- Orchestration del ripristino
  - Offre restore rapidi, flessibili e granulari per le VM
- Supporto della protezione con riconoscimento dell'applicazione per SQL con Transparent Snapshots
- Viste avanzate degli asset per le VM nella finestra Asset e policy
- Protezione parallela dei cluster Kubernetes

Sicurezza aggiornata

- Refresh dei certificati di terze parti
- Miglioramenti delle prestazioni della crittografia over-the-wire

Nuove funzionalità cloud

- Supporto di Oracle Cloud VMware Solution (OCVS)
- Supporto di Cloud DR per AWS nell'area APJ-Region-3

Controllo granulare

- Porte configurabili per gli agent applicativi
- Limiti di rallentamento configurabili per gli host degli agenti applicativi
- Supporto per le modifiche di IP DHCP dell'agent

Miglioramento dell'esperienza del cliente

- Configurazione del fuso orario dell'interfaccia utente
- Report tramite e-mail pianificati
- Stato di indicizzazione del motore di ricerca
- Passaggi dei processi di configurazione per gli agent applicativi

- Miglioramenti della verifica preliminare al flusso di lavoro degli aggiornamenti del sistema
- Processi avanzati per modifica dell'IP e sostituzione dello storage

Per ulteriori informazioni, leggere la presentazione Novità di PowerProtect Data Manager 19.14.

Novità di PowerProtect Data Manager 19.13 (marzo 2023)

Miglioramenti dei carichi di lavoro

- Oracle IncrementalMerge (OIM)
  - Fornisce backup a livello di immagine di Oracle
  - Offre accesso istantaneo e funzionalità di live mount
- Supporto dei backup federati di Oracle Data Guard
- NAS dinamico
  - Supporto di IPv6
  - Supporto di più VLAN per una maggiore flessibilità
- Aggiornamento agent standalone
  - Esecuzione congiunta dell'agent di Data Manager e l'agent standalone
- Supporto OS localizzato per asset (e origine asset)
- Ottimizzazione della memoria di sistema
- Cloud Snapshot Manager
  - Supporto per Google Cloud
  - Integrazione con il vault di Cyber Recovery in Azure (beta)
- Crittografia in esecuzione per la protezione delle VM

Sicurezza aggiornata

- 2FA per RSA SecurID
- Crittografia in esecuzione per la protezione delle VM

Funzionalità cloud migliorate

- Cloud Snapshot Manager
  - Supporto per Google Cloud
  - Integrazione con il vault di Cyber Recovery in Azure (beta)

Novità di PowerProtect Data Manager 19.12 (ottobre 2022)

Sviluppi dei carichi di lavoro

- Miglioramenti al NAS dinamico
  - Funzionalità PowerScale migliorata per supportare l'onboarding trasparente di PowerScale configurato con più zone di accesso e zone SmartConnect

        - Possibilità di scaricare i log degli elementi ignorati, visualizzare gli elementi ignorati di cui non è stato eseguito il backup tramite la protezione della condivisione NAS a causa di problemi di file o ACL e filtrare gli elementi ignorati a seconda della categoria di problema
    - Miglioramenti delle macchine virtuali
        - Aumento del numero di backup e restore simultanei di VM TSDM da 10 a 20, aumento del throughput e riduzione dei tempi di backup
        - vSphere Installation Bundle (VIB) è stato ottimizzato per rilevare se il software esiste già in un datastore e caricare così solo il VIB in cui il software non è condiviso tra gli host ESXi.
    - Supporto per Oracle Data Guard (solo standalone)
    - Miglioramenti di Kubernetes
        - Possibilità di aggiornare i campi di configurazione di PowerProtect Controller, Velero o cProxy, utilizzabili per aggiungere schede di interfaccia di rete (NIC) o impostare la configurazione DNS per i pod.

Maggiore sicurezza

- Il protocollo IPv6 è supportato dal core PowerProtect Data Manager, dagli agent delle applicazioni e dai backup delle macchine virtuali.
- Configurazione delle unità di storage e delle policy di protezione per abilitare il blocco della retention in modalità di conformità sul protection storage.

Esperienza del cliente facile da utilizzare

- Introduzione della finestra Job asset.
- Identificazione dei conflitti di pianificazione all'interno di una policy di protezione e modifica conseguente delle pianificazioni.
- Report e-mail

Novità di PowerProtect Data Manager 19.11 (giugno 2022)

Miglioramento dell'esperienza offerta al cliente

- Integrazione con Dell ISG Storage
    - Possibilità di snapshot dei PVC Kubernetes per lo stesso gruppo di volumi
    - Utilizzo dell'estensione di snapshot del gruppo di volumi del driver PowerFlex CSI
- Supporto per la protezione dei PVC sottoposti a provisioning in diverse zone di accesso PowerScale
    - Utilizzato per consentire o negare l'accesso ai volumi che risiedono in queste zone
- Supporto per la protezione centralizzata dei dati Oracle
- Supporto dell'agent di Oracle RMAN con Oracle 21c

- Possibilità di inviare gli aggiornamenti a tutti gli agenti dal server centrale PowerProtect Data Manager
- Supporto per la crittografia dei dati di backup e ripristino in-flight per gli asset cluster Kubernetes

Maggiore sicurezza

- Controllo degli accessi a livello di istanza RBAC
  - Controllo granulare degli asset
  - I clienti possono limitare le autorizzazioni a ciò che è necessario solo per la protezione dei dati
  - Protezione amministratore non richiesta
- Possibilità per gli account di sistema con diritti non amministrativi di rilevare, effettuare backup e ripristinare asset SQL

Funzionalità migliorata

- Replica del backup primario al completamento
- Supporto per l'inoltro del server syslog
- Possibilità di esportare le tabelle UI di PowerProtect Data Manager in CSV
- Miglioramenti del reporting on-premise

Novità di PowerProtect Data Manager 19.10 (marzo 2022)

Miglioramento dell'esperienza offerta al cliente

- Anteprima tecnica del reporting on-premise
  - Dashboard aggiornati: widget job, asset, integrità, conformità, capacità e ottimizzazione dello spazio
  - Report KPI dettagliati
    - Riepilogo delle protezioni degli asset
    - Job di backup, restore e replica
  - Possibilità di monitorare i processi self-service dalla console di PowerProtect Data Manager

Miglioramento di funzionalità e casi d'uso

- Miglioramenti del file system
  - Ripristino bare metal per l'intero sistema operativo Windows e i dati
  - Espansione delle piattaforme: Windows Server 2022 e AIX
  - Riconoscimento cluster Windows FS

        - Aggiunta un'opzione di visualizzazione dell'interfaccia utente per passare da una vista elenco di tutti gli asset del file system a una vista gerarchica degli asset all'interno di ciascun host del file system rilevato in Data Manager
    - Cloud
        - Mobility delle snapshot trasparenti VMware on-premise su cloud Azure o AWS per facilitare il ripristino di emergenza (DR) nel cloud
        - I backup archiviati in un pool di sistemi DD Smart Scale supportano Cloud DR
    - VMware
        - Prestazioni migliorate per Transparent Snapshots Data Manager (TSDM)
            - TSDM è stato ottimizzato per aumentare il restore throughput e soddisfare in modo più efficiente gli RTO delle VM
            - Le policy VM configurate con la modalità di ottimizzazione della capacità ora saranno in grado di utilizzare la protezione basata su TSDM
            - Supporto della VVOL
            - CDR abilitato per snapshot trasparenti
        - VM Restore
            - Sostituzione del controllo dell'account utente per Windows FLR
    - Miglioramenti alle applicazioni
        - Possibilità di inviare gli aggiornamenti a PowerProtect Data Manager 19.10 a tutti gli agent da un server PowerProtect Data Manager centrale, riducendo la necessità di aggiornamenti manuali singoli
        - Supporto host/agent per più FQDN

Integrazione Smart Scale

- PowerProtect Data Manager come applicazione di backup per Smart Scale
- Presentazione per i clienti di Smart Scale

Cyber Recovery e Cyber Sense

- Supporto del vaulting dei dati da MTree con Retention Lock Compliance
- Aumento delle prestazioni per la scansione di PowerProtect Data Manager Exchange

Novità di PowerProtect Data Manager 19.9 (settembre 2021)

Casi di utilizzo moderni

- Protezione centralizzata del database Oracle su AIX, incluso il supporto di Oracle-RMAN-Agent per AIX 7.1

- Supporto dei parametri avanzati Oracle per l'ottimizzazione delle prestazioni
- Kubernetes: utilizzo degli schemi di struttura in CRD

Casi di utilizzo di VMware

- **Istantanee trasparenti** (funzionalità di differenziazione chiave): Istantanee trasparenti è un nuovo metodo di immagine delle VM che tiene traccia delle modifiche man mano che si verificano, rimuovendo la latenza sperimentata durante un'istantanea. Con un nuovo data mover plug-in gestito che riduce la necessità di proxy esterni, PowerProtect Data Manager offre una protezione completa delle immagini delle VM per tutti i sistemi business-critical.
- La modifica delle impostazioni di rete delle VM durante il ripristino semplifica e accelera l'aggiornamento delle impostazioni di rete della VM durante il ripristino.
- Supporto della protezione delle VM PowerProtect Data Manager per Google Cloud VMware Engine

Cloud

- Cloud DR con il supporto di PowerProtect Data Manager per ambienti di rete privata in AWS e Azure
- Installazione più semplice di Data Manager e APEX Protection Storage in Azure Marketplace
- Copia delle snapshot in APEX Protection Storage in Azure per ridurre i costi di storage

Integrazione dello storage

- **Protezione NAS dinamica** (funzionalità di differenziazione chiave):la protezione NAS dinamica automatizza e ottimizza la protezione dell'infrastruttura NAS, offrendo un modo semplice e moderno per proteggere i sistemi NAS.

Facilità di manutenzione, disponibilità, TCE

- Miglioramenti dei processi e della facilità di manutenzione, tra cui:
- Supporto all'annullamento dei processi di protezione e ripristino per tutti gli application agent
- Supporto all'annullamento per processi vari (conformità, retention ad hoc, esportazione, ecc.)
- Possibilità di scaricare i registri end-to-end
- Fornisce log completi per il debug end-to-end
- Supporto delle eliminazioni degli asset e delle origini degli asset
- Messaggi di errore (EEMI) migliorati
- Esperienza utente migliorata nella gestione del ciclo di vita dei pacchetti di aggiornamento
- Supporto dei backup dei server su DDBoost
- Nuove viste degli asset native per SQL

Ripristino dopo un attacco informatico

- Supporto di configurazioni syslog centralizzate
- API REST nel Dell Marketplace

Ulteriori miglioramenti

- Tutti i documenti API sono ora disponibili su http://developer.dell.com
- Consentita la modifica dei criteri di protezione disabilitati
- Supporto alla scalabilità intelligente per pool di sistemi
- Disponibile una soluzione Hadoop per proteggere il database HBASE implementato nel cluster Hadoop.

Introduzione di PowerProtect Data Manager Essentials (giugno 2021)

PowerProtect Data Manager Essentials è un'offerta software per la protezione dei dati che condivide lo stesso set di funzionalità di PowerProtect Data Manager (Plus) con un prezzo massimo e un limite di capacità/socket destinato al mercato di fascia media. Alla base di questa nuova offerta c'è un nuovo servizio di implementazione ProDeploy. ProDeploy for PowerProtect Data Manager Essentials è un pacchetto di servizi di distribuzione dei componenti, destinati a soddisfare quel giusto equilibrio dei casi di utilizzo dei clienti di PowerProtect Data Manager Essentials. Per ulteriori informazioni sul nuovo servizio, cliccare qui.

Novità di PowerProtect Data Manager 19.8 (maggio 2021)

Cloud

- Integrazione di PowerProtect Cloud Snapshot Manager: PowerProtect Data Manager fornisce informazioni di riepilogo e avvisi da PowerProtect Cloud Snapshot Manager
- Il flusso di lavoro di implementazione integrato PowerProtect Data Manager + APEX Protection Storage AWS dal marketplace AWS offre un'esperienza pronta all'uso migliore e semplificata
- Cloud DR: raggiungimento di standard rigorosi per il programma AWS Storage Competency

VMware

- Certificazioni VMware: VMC, vSAN/vSphere, VCF
- Certificazione Data Manager 19.6: VMware Ready for vSphere/vSAN 6.7.x e 7.0
- Certificazione Data Manager 19.7: VMware Ready for vSphere/vSAN 7.0 U2; VMware Cloud on AWS M14
- Qualificazione di vSphere 7.0 U1 e U2 con il supporto Data Manager
- Certificazione Data Manager 19.7 VMware con VCF 4.2
- Il restore compresso di PowerProtect Data Domin per vProxy migliora l'RTO
- Ricerca e ripristino di file su più VM

Casi di utilizzo moderni

- Protezione Kubernetes: supporto della versione GA di Container Storage Interface per le istantanee
- Miglioramenti di vProtect
  - RBAC: ruoli predefiniti per amministratore/operatore
  - Backup completi e incrementali per i file Nutanix (AFS) con Changed File Tracking
  - Gestione delle istantanee di Ceph RBD
  - Miglioramenti all'integrazione dell'interfaccia utente di oVirt, RHV, OLVM
  - Miglioramenti alla presentazione dei dati
  - Configurazione guidata per backup oVirt, RHV, OLVM DB
- Backup e ripristino Hadoop di ACL con attributi estesi e dataset crittografati
- Multi-streaming per backup basati su file Windows e Linux
- Ripristino centralizzato di App Direct di SQL per più database dall'interfaccia utente di PowerProtect Data Manager

Cyber Recovery

- Vault di Cyber Recovery nel fattore di forma dell'appliance PowerProtect serie DP
- Rilevamento delle anomalie per i carichi di lavoro di PowerProtect Data Manager
- Telemetria Cyber Recovery: telemetria sicura basata solo su e-mail
- Supporto di più DDVE per Cyber Recovery in AWS

Facilità di manutenzione, disponibilità, TCE (ulteriori miglioramenti)

- Miglioramenti delle regole di policy: il refactoring dell'interfaccia utente delle policy fornisce più operazioni in un'unica regola di protezione
- Maggiore visibilità dei processi per il monitoraggio a livello di asset
- Gestione degli accessi - Aggiunta di più risorse di identità (LDAP/AD) per facilitare l'autenticazione
- SupportAssist migliora l'esperienza di supporto
- Ripristino automatizzato di PowerProtect Data Manager e del nodo di ricerca in caso di guasto irreparabile

Integrazione CloudIQ (aprile 2021)

L'integrazione di PowerProtect Data Manager con CloudIQ fornisce monitoraggio proattivo, analisi predittiva e informazioni approfondite per ridurre i rischi, pianificare in anticipo e migliorare la produttività attraverso una risoluzione dei problemi più rapida e tempi di risoluzione dei problemi più rapidi. Gli utenti di PowerProtect Central verranno reindirizzati a CloudIQ. Ulteriori informazioni sono contenute nella sezione "Monitoraggio e analisi basati su cloud" all'interno di questo documento.

Novità di PowerProtect Data Manager 19.7 (febbraio 2021)

Cloud

- Implementazione di Data Manager in Google Cloud. Facile implementazione da Google Marketplace. Supporta SQL, Oracle, SAP HANA, GKE
- Cloud Snapshot Manager: copia le istantanee AWS in PowerProtect DDVE
- Cloud Disaster Recovery: protezione e ripristino di VM più grandi e protezione per le regioni di Azure Government

Casi di utilizzo moderni

- Protezione Kubernetes
  - Protezione dei cluster guest Kubernetes in VMware Tanzu
  - Protezione delle risorse PaaS OpenShift
  - Protezione di GKE in esecuzione su Google Cloud
- Protezione Hadoop (tramite RPQ: protezione di più file, cluster più grandi)
- Miglioramenti di vProtect: supporto di DD Retention Lock, plug-in dell'interfaccia utente OpenStack, reporting di chargeback nell'interfaccia utente di vProtect

Casi di utilizzo di VMware

- Attivazione/disattivazione granulare della disattivazione su VMware/asset
- Automatizzazione della configurazione della protezione VCF

Cyber Recovery

- Implementazione del vault di Cyber Recovery in AWS
- Supporto DLm in Cyber Recovery Vault (da RPQ)
- Report sullo stato dei processi giornalieri

Miglioramento dell'esperienza offerta al cliente

- Miglioramenti della facilità di manutenzione dei job
- Opzioni di pianificazione flessibili nelle policy

Novità di PowerProtect Data Manager 19.6 (ottobre 2020)

- Implementazione di PowerProtect Data Manager in Azure, Azure Government e AWS GovCloud per la protezione dei carichi di lavoro in-cloud
- Gestione basata su policy di storage per le VM VMware
- Protezione di VMware Cloud Foundation
- Protezione senza agent coerente con le applicazioni di PostgreSQL e Cassandra in Kubernetes

- Protezione dei cluster Kubernetes in ambienti multicloud
- Backup delle risorse a livello di cluster Kubernetes
- Ripristino di SQL centralizzato con riconoscimento delle applicazioni
- Monitoraggio SaaS esteso
- Migliore resilienza
- Supporto per vRA 8.2

Novità di PowerProtect Data Manager 19.5

Protezione dei dati di carichi di lavoro in AWS

- Implementa PowerProtect Data Manager in AWS con automazione dal Marketplace AWS per proteggere carichi di lavoro business-critical nel cloud

Semplifica il consumo della protezione dei dati dell'hybrid cloud

- Ottieni una protezione completa dei dati sul cloud (retention a lungo termine, backup di Cloud Disaster Recovery su cloud e backup in scenari cloud) tramite abbonamento e in modo semplice e flessibile
- Supporto espanso di hypervisor con vProtect, che aggiunge il supporto per hypervisor Nutanix, oVert, ProxMox, Xen, Openstack, Oracle VM, RedHat, KVM, XCP-NG e per VM Oracle Linux
- Protegge Microsoft Exchange
- Integrated Data Protection Appliance per il protection storage di destinazione

Kubernetes

- Backup coerenti delle applicazioni per MySQL e MongoDB in esecuzione su Kubernetes
- Ripristino a un cluster Kubernetes alternativo

Reporting basato su SaaS migliorata

- Riepilogo della protezione degli asset delle ultime 24 ore
- Visualizzazione e dettagli della cronologia delle attività di protezione per ciascun asset protetto
- Riepilogo della protezione degli asset tramite una visualizzazione grafica dei criteri attuali per l'asset
- Riepilogo delle principali cause di errori degli asset, con dettagli degli errori che si verificano più spesso dopo il backup principale
- Report di audit, consolidamento dei registri audit da PowerProtect Data Manager nel tuo ambiente

Che cos'è PowerProtect Data Manager?

Che cos'è Dell PowerProtect Data Manager?

PowerProtect Data Manager è la soluzione di protezione dei dati per i moderni carichi di lavoro multicloud, comprese applicazioni di database, macchine virtuali (VM), contenitori Kubernetes e file system sia on-premise che nel cloud. PowerProtect Data Manager offre agli amministratori dei database (DBA) protezione e ripristino dei dati self-service tramite Application Direct (in precedenza DD Boost for Enteprise Applications). PowerProtect Data Manager fornisce la massima integrazione con VMware, supportando protezione VM e ripristini avanzati tramite proxy virtuali a prestazioni elevate. Insieme alla protezione dei dati, PowerProtect Data Manager offre servizi di protezione dei dati, tra cui conformità, governance, sicurezza, visibilità e analisi per i dati in gestione.

PowerProtect Data Manager sostituisce i prodotti Dell Data Protection esistenti?

No. PowerProtect Data Manager è complementare al portafoglio esistente di prodotti per la protezione dei dati. PowerProtect Data Manager non sostituisce i prodotti DP esistenti (Networker, Avamar, RecoverPoint for Virtual Machines, Cloud Snapshot Manager, ecc.). I clienti necessitano di soluzioni di protezione che supportino gli ambienti IT in continua evoluzione. Posizionare PowerProtect Data Manager quando:

- i clienti non dispongono di soluzioni Dell Data Protection
- i clienti dispongono di PowerProtect Data Domain, ma non dispongono di Data Protection Suite (Avamar e Networker)
- i clienti dispongono di PowerProtect Data Domain e Data Protection Suite (per l'aggiornamento o l'installazione legacy)
- Coesistenza: nei casi in cui i clienti dispongano di ambienti Avamar e abbiano anche la necessità di proteggere carichi di lavoro moderni, ad esempio Kubernetes. Coesistenza tramite Data Protection Central

Quali sono le caratteristiche e i vantaggi principali per i clienti di PowerProtect Data Manager?

Attributo	Vantaggi per i clienti
Soluzione definita dal software	Soluzione basata su software che si allinea direttamente con gli appliance fisici o virtuali Dell PowerProtect
Automazione e orchestration	Rilevamento e protezione automatizzati di database, virtual machine, file system e contenitori Kubernetes
Ottimizzazione multicloud	Supporto per tutti i casi di utilizzo per la protezione dei dati cloud: retention a lungo termine, ripristino di emergenza, backup sul cloud e in-cloud
Self-service	Consente ai proprietari dei dati di eseguire il backup e il ripristino direttamente dalle interfacce delle applicazioni native
Supervisione e governance centralizzate	Mitiga i rischi e assicura la conformità di SLA e SLO

Monitoraggio e analisi basati sul cloud	L'integrazione con APEX AIOps fornisce telemetria, apprendimento automatico e analisi predittiva per intraprendere azioni in modo proattivo e ridurre il tempo di risoluzione dei problemi.
Protezione efficiente	Protegge i dati direttamente negli appliance PowerProtect
Architettura moderna basata su servizi	Innovazione continua e modello di aggiornamento

Quali carichi di lavoro sono supportati con PowerProtect Data Manager?

PowerProtect Data Manager fornisce la gestione dei seguenti carichi di lavoro:

- Database: Oracle, SQL, SAP HANA, Exchange
- Cloud nativo: contenitori Kubernetes
- Protezione, ripristino e replica di macchine virtuali
- File system: Windows e Linux
- PowerProtect Data Manager è in grado di proteggere Oracle, SQL, SAP HANA, Kubernetes e macchine virtuali in esecuzione in VMC.
- La licenza di PowerProtect Data Manager può attivare Cloud Snapshot Manager, una soluzione SaaS che semplifica la protezione dei carichi di lavoro critici nel public cloud, sfruttando la tecnologia delle istantanee di base del provider cloud, senza necessità di installazione o infrastruttura.
- Nota: i seguenti carichi di lavoro sono supportati con le funzionalità PowerProtect Data Manager Application Direct e Storage Direct Protection: Hadoop, DB2, Exchange, SAP Hana, SAP per Oracle.

È in programma di supportare un maggior numero di carichi di lavoro nelle versioni future?

Sì (se il cliente necessita di assistenza per un carico di lavoro che non è attualmente supportato, richiedere un incontro con Product Management).

È necessario Dell Protection Storage per PowerProtect Data Manager?

Sì. PowerProtect Data Domain è una destinazione richiesta per PowerProtect Data Manager. In alternativa, PowerProtect Data Manager Appliance è disponibile anche come appliance integrata.

PowerProtect Data Manager viene eseguito nel cloud?

Sì. Poiché un numero sempre maggiore di aziende adotta una strategia multicloud, avvalersi di una soluzione comune per la protezione dei dati nell'infrastruttura locale e nel public cloud, consentirà loro di raggiungere l'efficienza operativa e di risparmiare sui costi. Per le aziende che hanno carichi di lavoro in esecuzione su AWS, Azure e Google Cloud e necessitano di backup e ripristini self-service dagli strumenti per applicazioni di livello enterprise, PowerProtect Data Manager ora fornisce protezione dei dati dei carichi di lavoro in AWS, AWS GovCloud, Azure, Azure Government e Google Cloud.

I proprietari e gli amministratori di dati ora possono implementare PowerProtect Data Manager in questi cloud con automazione dai Marketplace AWS, Azure e Google Cloud per proteggere

carichi di lavoro business-critical nel cloud. PowerProtect Data Manager consente la protezione dei carichi di lavoro tradizionali, tra cui Oracle, SQL, SAP HANA e file di sistema, nonché le applicazioni cloud native in esecuzione in contenitori Kubernetes o macchine virtuali in esecuzione in VMware Cloud (VMC).

Facili da installare e implementare dai Marketplace AWS, Azure e Google Cloud, PowerProtect Data Manager insieme ad APEX Protection Storage forniscono livelli di prestazioni e deduplica elevati, superiori rispetto a quanto offerto dai concorrenti presenti sul mercato.

Quali sono i clienti target?

Clienti che non dispongono di Dell Data Protection

i clienti dispongono di PowerProtect Data Domain, ma non dispongono di Data Protection Suite (Avamar e Networker)

i clienti dispongono di PowerProtect Data Domain e Data Protection Suite (per l'aggiornamento o l'installazione legacy)

Avamar e Networker sono inclusi/supportati con PowerProtect Data Manager?

No, Avamar e Networker sono inclusi e supportati in Data Protection Suite (vedi: Data Protection Suite Toolbox)

Funzionalità di PowerProtect Data Manager

Quali funzionalità compongono PowerProtect Data Manager?

- Interfaccia di gestione per automazione, orchestration e governance
- Monitoraggio e analisi basati su cloud tramite APEX AIOps
- Istantanee trasparenti: le Istantanee trasparenti semplificano i backup delle immagini delle VM offrendo un impatto quasi azzerato sulle VM per garantire la disponibilità di tutte le VM su larga scala senza interruzioni del business
- Replica delle macchine virtuali: replica e ripristino rapidi per ambienti virtualizzati
- Storage Direct Protection: percorso diretto tra lo storage Dell Tier 1 e Data Domain, aumenta le prestazioni di backup e ripristino
- Protezione NAS dinamica: automazione e ottimizzazione della protezione dell'infrastruttura NAS per ottenere SLA migliorati attraverso una gestione semplice ed efficiente del backup e del ripristino NAS
- Application Direct: abilita il backup e il ripristino self-service tra le applicazioni e PowerProtect Data Domain
- Protezione dei dati cloud**:** backup su cloud, backup nel cloud, retention a lungo termine e Cloud Disaster Recovery
- Protezione basata su SaaS tramite PowerProtect Cloud Snapshot Manager, che consente ai clienti di rilevare, coordinare e automatizzare la protezione dei carichi di lavoro su più cloud in base a policy per un backup e un ripristino di emergenza trasparenti

PowerProtect Data Manager

Qual è il valore complessivo di Dell PowerProtect Data Manager?

Dell PowerProtect Data Manager fornisce funzionalità di protezione dei dati per il Modern Data Center. Offre la protezione dei dati self-service e un'esperienza di backup centralizzata per le organizzazioni che stanno affrontando la trasformazione digitale in maniera semplice ed efficiente.

In particolare, grazie a Data Manager i clienti potranno:

- Automatizzare il provisioning dell'appliance PowerProtect Data Domain per abilitare i DBA con obiettivi di protezione as-a-service.
- Individuare e catalogare i backup eseguiti dagli amministratori IT (ad esempio, i DBA) in modalità self-service per misurare la conformità alla protezione rispetto agli obiettivi aziendali (ad esempio, RPO).
- Garantire la disponibilità di tutte le VM su larga scala senza interruzioni del business
- Automatizza e ottimizza la protezione dell'infrastruttura NAS
- Abilitare la protezione dei dati self-service con supervisione consolidata per ottimizzare l'attività di backup dei DBA e migliorare l'RTO per i database. Applicare l'esecuzione dei backup delle immagini delle VM per tali database tramite filtri dinamici.
- Consentire ai Compliance Administrator di eseguire il backup degli asset di VM, SQL, Oracle e file system.
- Creare una policy di protezione per eseguire automaticamente il backup, la replica e i tier di vari carichi di lavoro.
- Supporta tutti i casi di utilizzo per la protezione dei dati cloud: retention a lungo termine, cloud disaster recovery, backup sul cloud e in-cloud

In che modo PowerProtect Data Manager garantisce la protezione dei dati?

PowerProtect Data Manager abilita la protezione dei dati semplificando la creazione di policy che imposteranno la replica dei backup ed eseguendone anche il tier su cloud in base alla pianificazione scelta. Puoi impostare accordi sui livelli di servizio in base alle esigenze della tua organizzazione e PowerProtect Data Manager invierà una notifica qualora tali accordi non vengano soddisfatti.

In che modo PowerProtect Data Manager consente l'IT Transformation?

Per completare il modello self-service per i backup delle applicazioni, PowerProtect Data Manager estende il proprio paradigma di protezione per pianificare a livello centrale i backup dei database per SQL Boost Agent, Oracle RMAN Agent, virtual machine e file system dall'interfaccia utente di PowerProtect Data Manager. Ciò consente al team di backup di gestire in modo centralizzato le pianificazioni di backup complete, incrementali, differenziali e di log agevolando al contempo la transizione al team di DBA che potrebbe voler utilizzare Application Direct.

Quali sono i problemi che PowerProtect Data Manager è in grado di risolvere?

PowerProtect Data Manager fornisce alle organizzazioni strumenti semplici, rapidi ed efficienti per la protezione dei propri dati.

- Un Database Administrator può pianificare il backup per i propri asset.
- Un Backup Administrator può monitorare i backup eseguiti dai Database Administrator e pianificare i propri backup.

PowerProtect Data Manager semplifica il restore dei dati sottoposti a backup tramite VM live oppure nella posizione originale o in una alternativa. I dashboard informativi consentono all'utente di tenere traccia più facilmente dello stato di integrità dell'ambiente di protezione dei dati e di essere informati di qualsiasi problema; la deduplica globale riduce ampiamente i requisiti di rete e storage, mentre la tecnologia DD Boost garantisce backup di livello superiore.

Qual è il vantaggio offerto dalla supervisione consolidata di Dell PowerProtect Data Manager?

Grazie alla possibilità di gestire le operazioni di protezione decentralizzate che utilizzano risorse PowerProtect Data Domain, gli amministratori dei backup possono delegare attività di backup complesse ad altri membri del loro team, in modo da dedicare più tempo all'attività di innovazione. Gli amministratori di backup o conformità possono configurare PowerProtect Data Manager per definire in modo proattivo i Service Level Objectives e risolvere i potenziali problemi di conformità alla protezione.

Che cos'è Istantanee trasparenti?

Istantanee trasparenti, funzionalità disponibile con PowerProtect Data Manager 19.9, è un nuovo modo per proteggere ed eseguire il backup delle virtual machine VMware su larga scala senza compromessi indesiderati in termini di latenza, costo, scalabilità, prestazioni e complessità. Gli approcci tradizionali non sono riusciti a risolvere i problemi di interruzione del business durante i backup delle macchine virtuali, ma il software Istantanee trasparenti elimina questi ostacoli, rendendo le precedenti soluzioni di backup delle macchine virtuali obsolete. Semplificando e automatizzando i backup a livello di immagine delle VM con meno infrastruttura, le organizzazioni possono garantire la disponibilità dei dati delle VM in modo più efficace ed efficiente che mai. Istantanee trasparenti offre backup più rapidi e una riduzione della latenza delle VM.

Che cos'è Storage Direct Protection?

Storage Direct Protection, disponibile solo con Dell PowerProtect Data Manager, è una soluzione completa progettata per il backup e il ripristino rapidi, efficienti e sicuri dei dati su più cluster e snapshot locali. Offre:

- **Backup e ripristino rapidi**: riduzione al minimo della perdita di dati con RPO (Recovery Point Objectives) più brevi, grazie a rapide funzionalità di backup e ripristino in vari ambienti.
- **Protezione efficace dell'ecosistema**: ripristino perfetto delle piattaforme Dell Storage originali o alternative, con il supporto di un ecosistema più ampio e un'efficiente protezione dei dati.
- **Protezione dell'integrità dei dati**: protezione dei dati con funzioni immutabili e un cyber vault che garantisce una solida integrità dei dati.
- **Operazioni semplici**: gestione e orchestration centralizzate, rilevamento e protezione automatica di nuovi volumi, semplificando le operazioni quotidiane.

- **Supporto multicloud**: miglioramento della flessibilità con le funzionalità di replica e di cloud tiering di PowerProtect Data Domain, a garanzia di un'integrazione perfetta con gli ambienti multicloud.

Che cos'è la Protezione NAS dinamica?

La Protezione NAS dinamica, disponibile con PowerProtect Data Manager 19.9, offre una soluzione che affronta le sfide odierne dei clienti nella protezione degli ambienti NAS in continua evoluzione. Nello specifico, la Protezione NAS dinamica è indipendente dallo storage, rileva automaticamente gli asset NAS, offre backup incrementali perenni, fornisce l'utilizzo automatico e dinamico degli asset NAS con bilanciamento del carico e offre elaborazione scale-out automatica per l'ottimizzazione delle prestazioni. La Protezione NAS dinamica offre backup e ripristini più rapidi.

Che cos'è il rilevamento delle anomalie?

Il rilevamento delle anomalie utilizza l'apprendimento automatico per identificare rapidamente le attività sospette durante i backup nell'ambiente di produzione, garantendo sicurezza e integrità con un impatto minimo sulle risorse senza costi aggiuntivi.

- Valutazione **completa** dei metadati di backup per garantire l'integrità dell'infrastruttura digitale, migliorando l'uniformità operativa
- Il rilevamento **preventivo** delle anomalie fornisce informazioni rapide e sicure sui potenziali rischi per la sicurezza
- L'apprendimento automatico **proattivo** analizza i modelli per rilevare attività sospette, difendendo dalle minacce prima della loro escalation
- Rilevamento on-premise **leggero** all'interno di PowerProtect Data Manager

Ottimizzazione multicloud

Cos’è PowerProtect Cloud Tiering?

I clienti possono spostare i backup su un tier cloud dopo un certo periodo di tempo. Ciò consente ai clienti di ottenere il massimo dall'investimento in locale per la protection storage, mantenendo al contempo la conformità e la governance/retention dei backup sul cloud.

PowerProtect Cloud Tier consente di eseguire il tier di dati con protezione a lungo termine in uno storage cloud di un provider di cloud di propria scelta. È possibile specificare per quanto tempo un determinato backup di asset deve risiedere on-premise e PowerProtect Data Manager provvederà a spostare automaticamente i file al termine della durata indicata.

Quali cloud sono supportati con il PowerProtect Cloud Tier?

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

PowerProtect Data Manager può proteggere i carichi di lavoro nel cloud?

I clienti possono eseguire PowerProtect Data Manager in AWS, AWS GovCloud, Azure, Azure Government e Google Cloud e proteggere i seguenti carichi di lavoro: SQL, Oracle, SAP HANA, cluster Kubernetes e macchine virtuali in esecuzione in VMC.

Cloud Disaster Recovery è disponibile in PowerProtect Data Manager?

Sì, è stato introdotto dalla versione PowerProtect Data Manager 19.2 in poi.

Che cos'è Cloud Disaster Recovery?

Il Cloud Disaster Recovery (Cloud DR) consente alle aziende di copiare le macchine virtuali protette dagli ambienti di PowerProtect Data Manager allo storage a oggetti del public cloud e di orchestrare test di DR automatizzati, fail-over DR e failback dei carichi di lavoro di tier 2 al/dal cloud in uno scenario di emergenza. L'estensione della protezione dei dati esistente dalla sede del cliente al cloud offre un'esperienza utente familiare, richiedendo pertanto un livello minimo di formazione. I vantaggi aggiuntivi di Cloud DR includono un ingombro minimo del cloud durante le operazioni di routine e il ripristino orchestrato.

Quali cloud pubblici sono supportati con Cloud Disaster Recovery?

La protezione Cloud DR Protection è supportata su AWS e Azure Object Storage.
Cloud DR supporta il ripristino in caso di istanze di cloud nativi e il ripristino diretto a VMware Cloud on AWS o vCenter locale.

Quali sono i vantaggi di Cloud Disaster Recovery?

Protezione del cloud a costi contenuti: utilizza lo storage a oggetti e le risorse di elaborazione minime del cloud durante la protezione continua e risorse di elaborazione aggiuntive per le istanze recuperate on-demand quando è necessario il failover.

- Salva le copie delle macchine virtuali secondarie nello storage a oggetti cloud.
- Clicca 3 volte per ripristinare alle istanze native del cloud, VMware Cloud on AWS o per tornare a vCenter in locale.
- Clicca 2 volte per il failback dei carichi di lavoro in esecuzione nel public cloud AWS o Azure dopo un evento di failover.

Application Direct

Che cos'è Application Direct?

Con Application Direct, i proprietari di dati eseguono backup e ripristino direttamente dalle applicazioni native a PowerProtect Data Domain, APEX Protection Storage e serie DP o Integrated Data Protection Appliance, mentre PowerProtect Data Manager abilita supervisione e governance

Qual è la value proposition chiave di Application Direct?

- **Integrazione delle applicazioni:** Application Direct utilizza l'interfaccia di gestione delle applicazioni native per consentire ai proprietari delle applicazioni di proteggere i propri dati, direttamente al protection storage.
- **Mobilità dei dati ottimizzata:** Application Direct utilizza DD Boost come data mover. Questo consente l'elaborazione distribuita dei segmenti sul server delle applicazioni, inviando in rete solo dati univoci al PowerProtect Data Domain, consentendo un backup più rapido.

Quali agenti applicativi sono inclusi in PowerProtect Data Manager?

- Oracle: consente ai proprietari delle applicazioni di eseguire il backup direttamente e in tempi più rapidi tramite Oracle RMAN.
- Microsoft SQL Server: consente ai proprietari delle applicazioni di eseguire il backup in modo più rapido e direttamente da Microsoft SQL Server Management Studio.
- MS Exchange, file System (Windows & Linux), SAP HANA sono regolati utilizzando PowerProtect Data Manager.
- Il backup e il ripristino di SAP, Microsoft Exchange e IBM DB2 sono supportati da Application Direct, tuttavia non sono ancora gestiti da PowerProtect Data Manager. Il supporto per queste applicazioni verrà aggiunto in una versione successiva.

File System Agent

Che cos'è Application Direct File System Agent?

Analogamente agli agent delle applicazioni, Application Direct File System Agent aggiunge la possibilità di proteggere i file di sistema su host Windows e Linux.

Un amministratore di backup o di file system ora può eseguire il backup o il restore dei file system direttamente da PowerProtect Data Domain tramite PowerProtect Data Manager o utilizzando i comandi di backup e ripristino self-service.

Il Block Based Backup è supportato per File System Agent?

File System Agent supporta il backup basato su blocchi per eseguire ripristini e backup a livello di immagine.

Il File System Agent può essere installato come agent standalone per il backup e il ripristino di file system senza Data Manager?

No. Il File System Agent è necessario per la registrazione di PowerProtect Data Manager.

File System Agent supporta i ripristini a livello di file?

Sì, i ripristini a livello di file sono supportati da PowerProtect Data Manager. La funzionalità di ricerca e indicizzazione a livello di file sarà disponibile nelle prossime versioni.

Plug-in DDBoost File System (BoostFS)

BoostFS è incluso in PowerProtect Data Manager?

Sì

Quali sono i sistemi operativi supportati da BoostFS?

BoostFS supporta Linux e Windows. Per informazioni sulle specifiche varianti dei sistemi operativi Linux e Microsoft supportate, consulta le domande frequenti sulla protezione General Storage Direct.

Supporto di VMware e virtualizzazione

Contenuto del supporto VMware di PowerProtect Data Manager

PowerProtect Data Manager fornisce funzionalità di backup e ripristino delle immagini delle macchine virtuali coerenti con le applicazioni per numerose applicazioni comuni; inoltre, in futuro fornirà una serie di funzionalità self-service per gli amministratori di macchine virtuali. Ricerca di asset delle macchine virtuali che accelera la discovery dei dati da sottoporre a restore.

In che modo PowerProtect Data Manager semplifica e automatizza la protezione dei dati delle VM?

PowerProtect Data Manager è l'unica soluzione che offre l'integrazione di vSphere nativo con vCenter per la protezione delle VM, consentendo agli amministratori di storage e backup ed ai proprietari di VM di scegliere una policy di storage da applicare automaticamente a ogni VM quando viene istanziata. Questo si chiama anche gestione basata su policy dello storage VMware (Storage Policy-Based Management, o SPBM).

Che cos'è l'accesso istantaneo?

Accesso istantaneo è la possibilità di eseguire l'avvio di più macchine virtuali utilizzando una copia di protezione. Montare i dischi delle macchine virtuali (VMDK) sulla rete per l'esecuzione su PowerProtect Data Domain invece di eseguirne il restore in un sistema di storage primario separato.

- Evitare il costo dello storage di produzione durante il restore dei backup delle macchine virtuali.
- Eseguire lo staging dei restore di produzione.
- Ripristino a livello di file
- Accedere ai dati raw delle applicazioni necessari per eseguire analisi.
- Eseguire il restore "istantaneo" utilizzando VMware Storage vMotion o l'interfaccia utente di vCenter.

Quali sono i casi di utilizzo di Instant Access?

Instant Access offre un time-to-value superiore per i seguenti ruoli IT:

- I team DevOps eseguono in pochi secondi applicazioni o copie di produzione in esecuzione su PowerProtect Data Domain come sandbox di test e sviluppo.
- I team di analisti aziendali possono eseguire analisi su una copia di un database dell'applicazione di produzione.
- Gli Storage Administrator e i Backup Administrator possono gestire sessioni di accesso istantaneo e noleggiare, estendere o recuperare I/O casuali utilizzati dall'attività di restore istantaneo o delle VM live.
- I DBA possono ridurre al minimo il downtime grazie alla possibilità di eseguire il mounting di VMDK tramite il ripristino di SQL Server Management Studio. Ogni backup delle immagini delle VM con riconoscimento dell'applicazione per SQL Server installa

automaticamente SQL Server Management Studio, Dell Microsoft Application Agent e Dell ItemPoint.

Quali sono gli aspetti importanti dei backup delle immagini con riconoscimento dell'applicazione rispetto ai backup coerenti con le applicazioni?

Uno degli elementi più importanti del riconoscimento delle applicazioni virtualizzate è il trattamento delle loro specifiche esigenze di protezione dei dati. Una soluzione di base per la creazione di immagini delle VM coerente con le applicazioni si limita a disattivare un'applicazione senza eseguire ulteriori attività.

I backup con riconoscimento dell'applicazione di PowerProtect includono Dell Microsoft Application Agent come parte del processo di backup. In questo modo i backup dei log, il troncamento dei log e l'installazione di un agent di protezione per SQL Server Management Studio consentono ai DBA di eseguire le attività di protezione automatica e ripristino dei database.

VSphere è supportato da PowerProtect Data Manager

Sì

Qual è il vantaggio del supporto per vSphere?

Self-Service: ripristino delle risorse della macchina virtuale direttamente all'interno di vSphere
Gli utenti non devono lasciare bisogno di lasciare il proprio "strumento di scelta" per la gestione della protezione dei dati. Gli strumenti di ripristino sono accessibili nello stesso IDE in cui è gestito l'ambiente della macchina virtuale.

Quali hypervisor supporta PowerProtect Data Manager?

Oltre a VMware, PowerProtect Data Manager supporta diversi hypervisor tramite vProtect. L'aggiunta di vProtect a PowerProtect Data Manager estende il supporto dell'ambiente virtuale da un'unica offerta, tra cui AWS EC2, AHV, RHEV, Oracle Virtualization Manager, hypervisor Citrix, Xen e altri ancora. Gli amministratori sono abilitati con gestione delle istantanee e del ripristino e backup completi e incrementali a livello di macchine virtuali e senza agent coerenti con le applicazioni. vProtect è integrato con PowerProtect Data Domain tramite BoostFS per la lettura/scrittura diretta.

Che cos'è la virtualizzazione OpenShift?

La virtualizzazione OpenShift, con KubeVirt, è una tecnologia che estende la funzionalità Kubernetes per supportare e gestire le macchine virtuali (VM) insieme ai carichi di lavoro containerizzati all'interno dello stesso ambiente. In questo modo le aziende possono integrare e gestire in modo efficiente applicazioni legacy o non containerizzate all'interno dei cluster Kubernetes.

Perché i clienti desiderano la virtualizzazione OpenShift?

Molti clienti utilizzano applicazioni che non possono essere facilmente containerizzate, ma richiedono comunque una gestione e una protezione dei dati affidabili. La virtualizzazione OpenShift colma questo divario consentendo alle organizzazioni di:

- Proteggere le VM Linux e Windows direttamente negli ambienti Kubernetes.
- Sfruttare un approccio open source standardizzato (KubeVirt) senza dover fare affidamento su soluzioni proprietarie.

- Semplificare la gestione integrando VM e container in un sistema unificato.

Questa soluzione è particolarmente interessante per i settori che dipendono da OpenShift, come quello delle telecomunicazioni, e per le organizzazioni che sono alla ricerca di soluzioni hypervisor alternative a causa di problemi legati a costi e licenze.

Quali funzioni sono disponibili nella versione PowerProtect Data Manager 19.19 relativa alla virtualizzazione OpenShift?

Le funzioni disponibili per la versione iniziale del supporto della virtualizzazione OpenShift in PowerProtect Data Manager 19.19 includono:

- Protezione iniziale dell'immagine delle macchine virtuali tramite PowerProtect Data Manager integrato con Kubernetes.
- Flussi di lavoro di backup e ripristino pari a quelli della protezione dei namespace/volumi persistenti (PV):
  - Flussi di lavoro Ripristina su nuova posizione e Ripristina su posizione alternativa.
  - Supporto per file system e storage a blocchi.
  - Disattivazione delle macchine virtuali per garantire la coerenza dei file system (congelamento/scongelamento).
- Individuazione delle macchine virtuali all'interno dei cluster Kubernetes.
- Scalabilità e prestazioni limitate.
- Data mover dello storage a blocchi per prestazioni di backup migliorate.
- Mappatura da namespace a macchine virtuali tramite un'interfaccia utente di facile utilizzo.

Quali vantaggi offre questa funzione agli utenti?

La virtualizzazione OpenShift offre un valore elevato, tra cui:

- **Protezione end-to-end dei dati Kubernetes**: proteggi i carichi di lavoro sia containerizzati che non containerizzati all'interno dei cluster Kubernetes.
- **Gestione completa**: fornisci un'unica piattaforma per gestire sia le macchine virtuali che le applicazioni Kubernetes.
- **Alternative VMware**: i clienti che esplorano possibili alternative alle piattaforme hypervisor tradizionali (ad esempio VMware) possono ridurre i costi e modernizzare l'infrastruttura.
- **Compatibilità tra piattaforme**: sfrutta una soluzione standardizzata (non proprietaria), garantendo il supporto futuro e un'ampia compatibilità dell'ecosistema.

Questa funzione offre una gestione e una protezione ottimali per i carichi di lavoro ibridi, fornendo alle organizzazioni gli strumenti per essere sempre agili e competitive.

Quali funzionalità sono previste per le versioni future del supporto della virtualizzazione OpenShift in PowerProtect Data Manager?

Gli aggiornamenti futuri includono:

- Differenziazione delle macchine virtuali all'interno dell'interfaccia utente di PowerProtect Data Manager.

- Casi d'uso di ripristino avanzato, come accensione/spegnimento, rete e annotazioni K8s.
- Modelli di applicazioni per database come MySQL, MongoDB, PostgreSQL e Cassandra.
- Casi d'uso estesi:
  - Ripristino a livello di file.
  - Migrazione delle macchine virtuali (equivalente di vMotion) all'interno di Kubernetes.
  - Accesso/ripristino immediati per le macchine virtuali.
- Supporto per SUSE Harvester e funzionalità Kubernetes aggiuntive come snapshot del gruppo di volumi.
- Ripristino di emergenza (DR) e pianificazione di failover/failback.

Questi miglioramenti offriranno funzionalità e scalabilità persino maggiori, in modo tale che PowerProtect Data Manager sia in grado di soddisfare requisiti aziendali complessi e su larga scala.

Supporto di hypervisor Hyper-V

Che cos'è l'agent di protezione Hyper-V?

L'agent di protezione Hyper-V è una nuova funzionalità di PowerProtect Data Manager, pensata appositamente per proteggere gli ambienti Hyper-V. Progettato da zero, questo miglioramento offre una protezione dei dati affidabile e cyber-resiliente per i carichi di lavoro Hyper-V.

Vantaggi principali

- Hyper-V Resilient Change Tracking (RCT) per backup per sempre incrementali, gestiti come backup sintetici completi.
- Funzionalità di ripristino completo delle macchine virtuali.
- Supporto della protezione Azure Stack HCI (ora Azure Local), completamente in linea con le configurazioni back-end Hyper-V.
- Dotato di certificazione con le policy supplementari Dell Windows Defender Application Control (WDAC).

Quali funzionalità sono incluse al momento del lancio?

Le seguenti funzionalità saranno disponibili a partire dalla versione iniziale di PowerProtect Data Manager 19.19 con supporto Hyper-V:

- Onboarding dei server Hyper-V in PowerProtect Data Manager.
- Individuazione dell'origine degli asset e degli asset stessi.
- Configurazione e creazione di policy.
- Backup completi delle macchine virtuali e backup incrementali.
- Ripristino completo a livello di immagine delle macchine virtuali.
- Protezione Azure Local (in precedenza Azure Stack HCI).

Quali miglioramenti offre questo aggiornamento rispetto a NetWorker o Avamar?

L'agent di protezione Hyper-V offre miglioramenti significativi rispetto a NetWorker e Avamar, ad esempio:

- Scalabilità e prestazioni migliorate con funzionalità come il multi-streaming.
- Supporto diretto per Windows Defender Application Control (WDAC), non disponibile in NetWorker e Avamar.
- Maggiori velocità di backup e ripristino, con prestazioni tecniche preliminari che misurano 14 TB/h per i backup e 1 TB/h per i ripristini.
- Proxyless Deployment e Push Agent Installation offrono un'esperienza quasi senza agent

Quali sono le limitazioni presenti al momento del lancio?

Sebbene la versione iniziale aggiunga solide funzionalità, vi sono alcune limitazioni da tenere in considerazione:

- Nessun accesso istantaneo e nessuna ricerca indicizzata per il ripristino al momento del lancio, ma questi miglioramenti sono presenti nella roadmap.
- Inizialmente non è supportato alcun database SQL o con riconoscimento delle applicazioni, ma ne è prevista l'aggiunta nelle versioni future.
- La piattaforma Azure Cloud (APEX) per Microsoft Azure non è supportata.

In che modo ciò migliora il supporto per Azure Local (in precedenza Azure Stack HCI)?

Il nuovo agent protegge completamente gli ambienti Azure Local utilizzando la stessa configurazione dei back-end Hyper-V. Ciò garantisce l'integrazione perfetta per le organizzazioni che utilizzano Azure Local per l'infrastruttura on-premise.

Perché il supporto delle piattaforme non VMware è importante?

È fondamentale espandere il supporto al di là di VMware, poiché molte aziende diversificano i propri ambienti hypervisor. Hyper-V, virtualizzazione OpenShift, Nutanix AHV e OpenStack/KVM sono le principali soluzioni preferite dai clienti che abbandonano VMware. Il supporto più ampio delle piattaforme fa sì che PowerProtect Data Manager sia sempre rilevante nel mercato in continua evoluzione.

Quali funzionalità sono previste per gli aggiornamenti futuri?

Le versioni future di PowerProtect Data Manager includeranno funzionalità aggiuntive, come:

- Accesso istantaneo e ricerca indicizzata per ripristini più rapidi.
- Ripristino a livello di file direttamente tramite l'interfaccia utente.
- Supporto SQL e con riconoscimento delle applicazioni.
- Operazioni a livello di disco come filtri di esclusione dei dischi di backup e ripristino a livello di disco.

Protezione Storage Direct

Che cos'è la tecnologia Protezione Storage Direct?

La Protezione Storage Direct incrementa Application Direct fornendo un percorso diretto dallo storage primario a PowerProtect Data Domain. Elimina l'impatto del backup sugli application server.

Qual è il valore per il cliente per la Protezione Storage Direct?

Molti clienti hanno ancora difficoltà a soddisfare i requisiti di protezione dei dati, in particolare per database e applicazioni mission-critical. Raggiungi i rigidi requisiti SLA, mantieni le prestazioni e fornisci copertura 24/7/365.

Quali sono le principali piattaforme di storage di Dell supportate dalla Protezione Storage Direct?

VMAX3, VMAX All Flash, PowerMax, PowerStore

Quali appliance PowerProtect Data Domain sono supportati dalla Protezione Storage Direct di PowerProtect Data Manager?

Per ulteriori informazioni, consulta la guida completa alla compatibilità di Data Manager qui.

Quali applicazioni supportano la Protezione Storage Direct a livello nativo?

L'application agent abilita il supporto nativo per:

- EPIC su Linux
- File system Linux

Protezione Storage Direct con Dell Storage

Quali sono i principali vantaggi dell'integrazione di PowerProtect Data Manager?

- Impatto zero sull'host durante il backup/ripristino. Il backup viene eseguito direttamente su PowerStore o tramite proxy su PowerMax senza consumare risorse da un host
- La protezione dei dati di Dell offre una strategia di backup incrementale perenne, con meno dati da leggere e trasferire via cavo al protection storage
- PowerProtect Data Manager è in grado di gestire snapshot PowerStore locali (ad esempio, ogni 30 minuti) e nello stesso backup della policy in PowerProtect Data Domain (1 volta al giorno)
- Il supporto delle snapshot locali per PowerMax sarà disponibile entro la fine dell'anno
- Più volumi da cluster PowerStore identici o multipli possono essere protetti con un unico backup manager

Quali sono i componenti principali di questa integrazione?

- PowerStore comunica direttamente con PowerProtect Data Domain su LAN tramite agente integrato e protocollo DDBoost
- Il backup di PowerMax viene eseguito sul proxy
- PowerStore o PowerMax offre il trasferimento di blocchi modificati, in cui è necessario trasferire solo blocchi di dati univoci tra PowerStore e PowerProtect Data Domain

- PowerProtect Data Manager funge da motore di orchestrazione tra PowerStore e PowerProtect Data Domain

Quali modelli Dell Storage sono supportati?

- Solo PowerMax 4 (2500/8500)
- Tutti i modelli PowerStore T da 500T fino a 9200T
- Per ulteriori informazioni, consulta la Guida alla compatibilità di PowerProtect Data Manager completa

Quando sarà disponibile la Protezione Storage Direct con Dell Storage?

- La Protezione Storage Direct con PowerStore e PowerMax è ora disponibile

Quali modelli PowerProtect Data Domain sono supportati?

- Tutti i modelli PowerProtect Data Domain, supportati da PowerProtect Data Manager
- APEX Protection Storage on-premise e nel public cloud (AWS)
- Per ulteriori informazioni, consulta la Guida alla compatibilità di PowerProtect Data Manager completa

Quali sono i possibili metodi di protezione?

- Snapshot PowerStore locale sull'array primario
- Snapshot PowerStore locale sull'array primario e snapshot remoto sull'array di replica
- Backup su PowerProtect Data Domain tramite array primario
- Backup su PowerProtect Data Domain tramite array di replica
- Replica di copie PowerProtect Data Domain
- Retention a lungo termine tramite il tiering su un cloud storage
- Il supporto delle snapshot locali per PowerMax sarà disponibile entro la fine dell'anno

Quali sono i possibili metodi di restore?

- Restore incrementale sul volume PowerStore originale o alternativo
- PowerMax supporta solo il restore completo
- Restore in un cluster diverso o nuovo in un sistema simile (ad esempio, da PowerStore a PowerStore, da PowerMax a PowerMax)
- Nessun supporto per i ripristini su più piattaforme (ad esempio, da PowerStore a PowerMax e viceversa)
- Accesso istantaneo all'host o al gruppo di host per PowerStore
- L'accesso istantaneo a PowerMax sarà disponibile in una versione successiva
- Restore da una copia Cloud Tier e da un Data Domain di replica
- Restore da snapshot PowerStore a volumi originali o di clonazione

- Il supporto delle snapshot locali per PowerMax sarà disponibile entro la fine dell'anno

È possibile proteggere i volumi di blocchi PowerStore o PowerMax e le condivisioni NAS?

- Sì, PowerProtect Data Manager supporta già la protezione delle condivisioni NAS di PowerStore
- PowerMax può essere protetto come share generica
- Questa nuova integrazione sta migliorando la capacità di consentire anche la protezione di volumi di blocchi e gruppi di volumi

Quali sono le funzionalità comuni di PowerProtect Data Manager supportate da questa integrazione?

- Pianificazione delle policy di protezione dei job
- Crittografia in trasferimento e supporto crittografia a livello di destinazione Data Domain
- Integrazione di DD Retention Lock (modalità governance, modalità conformità)
- Supporto di repliche DD
- Supporto di Cloud Tiering DD
- Supporto di regole dinamiche per PowerStore
- Il supporto delle regole dinamiche per PowerMax sarà disponibile in una versione futura

Possiamo condividere lo stesso appliance PowerProtect Data Domain con altri carichi di lavoro/applicazioni?

- Sì, lo stesso appliance di destinazione può essere utilizzato come destinazione per i backup di PowerStore o PowerMax e altri carichi di lavoro/applicazioni (basati su Data Manager, NetWorker, Avamar e terze parti)
- Per ulteriori informazioni, consulta la Guida alla compatibilità di PowerProtect Data Manager completa

Ulteriori dettagli sono disponibili nel blog dell'annuncio, nelle domande frequenti su Dell PowerStore, nel solution brief di PowerMax e nella pagina SharePoint di PowerStore 3.5

Rilevamento di anomalie

Che cos'è il rilevamento delle anomalie?

Il rilevamento delle anomalie è una funzione avanzata di PowerProtect Data Manager che offre il monitoraggio in seguito al processo di backup per rilevare potenziali minacce alla sicurezza, come i ransomware. Individuando le anomalie, avvisa gli utenti della presenza di attività sospette, in modo che le organizzazioni possano rispondere rapidamente ed efficacemente per proteggere i loro dati.

Come funziona il rilevamento delle anomalie?

Il rilevamento delle anomalie utilizza algoritmi sviluppati da Dell per monitorare i backup in tempo reale. Utilizza tre metodi fondamentali per rilevare le minacce:

- **Pattern matching**: confronta i metadati dei file (nomi, estensioni, percorsi) con una libreria di oltre 5.000 modelli noti di ransomware per identificare i rischi.
- **Analisi comportamentale**: analizza le tendenze utilizzando l'apprendimento automatico, ad esempio le modifiche all'utilizzo dei dati o la crittografia improvvisa dei file, per rilevare attività insolite utilizzando modelli di serie temporali.
- **Analisi della configurazione del sistema**: esegue la scansione delle impostazioni di configurazione del sistema (ad esempio, firewall, controlli degli accessi) per individuare le vulnerabilità che potrebbero essere sfruttate dai ransomware.

Una volta rilevate le anomalie, emette automaticamente degli avvisi e offre la possibilità di mettere in quarantena i dati potenzialmente dannosi per poter svolgere ulteriori indagini.
È importante tenere presente che per il corretto funzionamento del rilevamento delle anomalie, è necessario abilitare la ricerca e l'indicizzazione.

Quali sono i vantaggi derivanti dall'utilizzo del rilevamento delle anomalie?

Il rilevamento delle anomalie offre diversi vantaggi fondamentali:

- **Rilevamento tempestivo delle minacce**: identifica rapidamente i problemi prima della loro escalation, in modo che gli utenti possano reagire in modo proattivo.
- **Impatto leggero**: opera direttamente all'interno dell'ambiente di produzione senza utilizzare risorse aggiuntive dell'infrastruttura.
- **Avvisi in tempo reale**: fornisce notifiche immediate delle anomalie, in modo da poter prendere le decisioni in modo più rapido.
- **Nessun costo aggiuntivo**: incluso con PowerProtect Data Manager senza costi aggiuntivi.

Come funzionano insieme il rilevamento delle anomalie e CyberSense?

Il rilevamento delle anomalie e CyberSense costituiscono un duo potente per la cyber-resilienza. Il rilevamento delle anomalie opera all'interno dell'ambiente di produzione per individuare le minacce durante il processo di backup, mentre CyberSense fornisce analisi forensi approfondite dei dati isolati archiviati in un vault Cyber Recovery. CyberSense sfrutta l'apprendimento automatico basato sull'AI per convalidare l'integrità dei dati con una precisione del 99,99% e fornisce rapporti dettagliati sui file corrotti. Insieme, queste funzionalità creano una strategia di difesa a più livelli. Il rilevamento delle anomalie offre informazioni dettagliate immediate, mentre CyberSense garantisce ripristini intelligenti in caso di attacco informatico.

In che modo il sistema avvisa gli utenti delle anomalie?

Il rilevamento delle anomalie utilizza l'engine di reporting nativo di PowerProtect Data Manager per fornire avvisi critici e report aggiuntivi. Gli avvisi sono collegati a copie di backup specifiche tramite il collegamento "Visualizza copia", in modo che gli utenti possano indagare rapidamente sui dati segnalati. Ulteriori report, tra cui una pagina dedicata agli eventi correlati alla sicurezza, saranno disponibili nei prossimi aggiornamenti.

L'utilizzo del rilevamento delle anomalie comporta costi aggiuntivi?

No, il rilevamento delle anomalie è incluso in PowerProtect Data Manager senza costi aggiuntivi. Opera in modo nativo all'interno dell'infrastruttura on-premise senza richiedere strumenti o risorse di terze parti.

Perché i clienti dovrebbero utilizzare il rilevamento delle anomalie?

Il rilevamento delle anomalie aggiunge un livello proattivo di sicurezza a PowerProtect Data Manager, fornendo alle aziende gli strumenti per individuare e mitigare tempestivamente i rischi

informatici. Supporta la continuità aziendale, garantisce l'integrità dei dati e riduce l'impatto di potenziali violazioni. In combinazione con CyberSense e le funzionalità immutabili di PowerProtect Data Domain, il rilevamento delle anomalie offre una solida soluzione end-to-end di cyber-resilienza per gli ambienti aziendali.

Archiviazione a oggetti

Che cos'è l'archiviazione a oggetti?

L'archiviazione a oggetti è una nuova funzione di PowerProtect Data Manager 19.19 progettata per semplificare la retention dei dati a lungo termine archiviando i backup completi direttamente nello storage a oggetti, come Dell ECS o lo storage a oggetti basato su cloud, senza costi aggiuntivi per le licenze. È ottimizzato per la scalabilità, la flessibilità e per soddisfare le esigenze in termini di governance o conformità.

Quali sono i principali vantaggi dell'archiviazione a oggetti?

- **Archiviazione efficiente**: i flussi di lavoro automatizzati basati su policy riducono le attività manuali per le esigenze di retention a lungo termine.
- **Ripristini flessibili**: rende possibili i ripristini diretti dallo storage a oggetti senza routing tramite Data Domain, risparmiando tempo e semplificando i processi.
- **Storage scalabile**: supporta carichi di lavoro sostanziali, con un massimo di 200 TB archiviati ogni giorno e 1 PB ogni settimana.
- **Costi contenuti**: disponibile senza costi aggiuntivi per gli utenti di PowerProtect Data Manager (pagamento solo per lo storage ECS).

Come funziona l'archiviazione a oggetti?

- Archivia i backup completi da PowerProtect Data Domain allo storage a oggetti tramite un engine di protezione.
- I metadati vengono archiviati in un repository di oggetti per supportare il ripristino fluido dei dati.
- I ripristini possono essere eseguiti direttamente sulla destinazione di ripristino, eliminando la dipendenza da Data Domain per i ripristini.

Quali sono i principali casi d'uso per l'archiviazione a oggetti?

- **Governance e conformità**: semplifica la retention a lungo termine per soddisfare i requisiti normativi.
- **Cyber-resilienza**: backup di sicurezza secondario per lo storage a oggetti per una maggiore sicurezza del ripristino.
- **Archiviazione scalabile**: gestisci in modo efficiente le esigenze di archiviazione dei dati su larga scala.

Quali carichi di lavoro sono supportati dall'archiviazione a oggetti?

Il supporto iniziale include:

- Backup VMware (Transparent Snapshots e basato su VADP).
- Backup dei file system (FBB) per Linux e Windows.

Nelle versioni successive seguiranno il supporto pianificato per i backup incrementali, i file system aggiuntivi e carichi di lavoro come i backup di database.

Qual è la differenza tra archiviazione a oggetti e Cloud Tier?

- **Flessibilità**: con l'archiviazione a oggetti è possibile eseguire ripristini diretti sulle destinazioni di ripristino, mentre Cloud Tier richiede prima ripristini su Data Domain.
- **Limiti giornalieri/settimanali**: l'archiviazione a oggetti supporta un throughput più elevato (200 TB/giorno, 1 PB/settimana) rispetto a Cloud Tier.
- **Compressione**: l'archiviazione a oggetti comprime i dati ma non deduplica come Cloud Tier.
- **Copia di backup**: l'archiviazione a oggetti crea una seconda copia, promuovendo la cyber-resilienza, mentre Cloud Tier esegue la migrazione dei dati.

Esistono limitazioni con l'archiviazione a oggetti?

- Attualmente supporta solo macchine virtuali e file system VMware. Verrà estesa a ulteriori casi d'uso nelle prossime versioni.
- Il supporto iniziale è limitato a Dell ECS. AWS, Google Cloud e Azure verranno aggiunti in un secondo momento.
- Sono supportati i backup completi. I backup incrementali sono progettati per la versione 19.20.
- Nessun indice dei contenuti archiviati, che richiede il ripristino completo del backup per il ripristino di file specifici.
- I ripristini della cache e indicizzati sono pianificati per gli aggiornamenti futuri.

Reporting multi-sistema

Che cos'è il reporting multi-sistema?

Il reporting multi-sistema è una nuova funzionalità all'interno di PowerProtect Data Manager 19.19 che offre monitoraggio e reporting centralizzati per un massimo di 150 sistemi. Combina punti dati fondamentali, come processi, copie, avvisi e integrità del sistema, in un'unica interfaccia intuitiva, riducendo la complessità e migliorando l'efficienza operativa.

Quali sono le funzionalità principali del reporting multi-sistema?

- **Monitoraggio centralizzato**: gestisci fino a 150 istanze di PowerProtect Data Manager o PowerProtect Data Manager Appliance da un'unica console.
- **Reporting completo**: ottieni informazioni dettagliate su processi, storage, avvisi, audit log, integrità del sistema e altro ancora.
- **Dashboard personalizzabili**: inizia con modelli pronti all'uso o crea dashboard personalizzati specifici per le tue esigenze.
- **Strumenti di reporting avanzati**: sfrutta le funzionalità di livello enterprise di Grafana come pianificazione, Single Sign-On (SSO) e supporto multi-tenancy.
- **Retention dei dati**: conserva i dati cronologici fino a 18 mesi con la gestione automatica della retention per una visibilità completa.
- **Progettazione orientata al futuro**: pensato per integrare prodotti aggiuntivi nello stesso framework di monitoraggio e reporting.

In che modo il reporting multi-sistema migliora l'efficienza per i clienti?

Il reporting multi-sistema semplifica la gestione consolidando le informazioni provenienti da più sistemi in un'unica interfaccia. Gli amministratori IT possono ridurre il tempo impiegato per passare da un sistema all'altro e concentrarsi invece sui dati fruibili per prendere decisioni migliori e più rapide. Con funzionalità avanzate come dashboard personalizzabili e strumenti

Grafana, gli utenti possono personalizzare la propria esperienza per soddisfare esigenze aziendali specifiche, aumentando ulteriormente l'efficienza.

È possibile personalizzare i dashboard e i report nel reporting multi-sistema?

Sì. Il reporting multi-sistema fornisce modelli di dashboard pre-progettati per iniziare rapidamente. Gli utenti possono anche personalizzare i dashboard esistenti o crearne di nuovi per soddisfare requisiti operativi specifici. Gli utenti hanno inoltre la possibilità di accedere direttamente al database per query ad hoc e integrazione con strumenti specifici del cliente.

In che modo il reporting multi-sistema gestisce i dati cronologici?

Il reporting multi-sistema conserva i dati cronologici fino a 18 mesi per impostazione predefinita, con la gestione automatica della retention per mantenere le informazioni pertinenti e organizzate senza ulteriori sforzi.

Quali sono i piani di sviluppo futuro per il reporting multi-sistema?

Gli aggiornamenti futuri mirano a espandere le funzionalità di reporting multi-sistema, tra cui integrazioni più approfondite con ulteriori prodotti Dell Data Protection e funzionalità migliorate per la gestione proattiva e l'analisi avanzata.

Monitoraggio e analisi basati sul cloud

Che cos'è PowerProtect Central?

A partire da aprile 2021, Dell APEX AIOps (in precedenza CloudIQ) sostituirà PowerProtect Central per fornire monitoraggio e analisi basati su cloud per PowerProtect Data Manager. Gli utenti di PowerProtect Central verranno reindirizzati ad APEX AIOps.

Che cos'è APEX AIOps e cosa offre ai clienti di PowerProtect Data Manager:

APEX AIOps (in precedenza CloudIQ) fornisce telemetria, apprendimento automatico e analisi predittiva per intraprendere azioni in modo proattivo e ridurre il tempo di risoluzione dei problemi. Nello specifico, per ogni istanza di PowerProtect Data Manager, APEX AIOps fornirà le seguenti funzionalità:

- Riepilogo della protezione dei dati
- Report sulla protezione degli asset
- Dettagli della protezione degli asset
- Reporting sulla conformità degli asset
- Dettagli configurazione
- Avvisi

Ulteriori dettagli sono disponibili in Dell APEX AIOps-PowerProtect Knowledge Center e nella pagina Web AIOPs APEX.

Protezione basata su SaaS di carichi di lavoro nel cloud

Che cos'è Cloud Snapshot Manager?

PowerProtect Cloud Snapshot Manager è una soluzione SaaS che semplifica la protezione dei carichi di lavoro critici nel public cloud, sfruttando la tecnologia delle istantanee di base del provider cloud, senza richiedere installazione o infrastruttura. I clienti possono rilevare, coordinare e automatizzare la protezione dei carichi di lavoro in AWS e Azure con policy basate su etichette. I clienti possono attivare Cloud Snapshot Manager utilizzando la licenza di PowerProtect Data Manager.

Quali funzionalità sono disponibili grazie all'integrazione di Cloud Snapshot Manager con PowerProtect Data Manager?

Gli avvisi di PowerProtect Data Manager ora mostrano gli eventi di Cloud Snapshot Manager, incluso un riepilogo degli avvisi. All'interno di Data Manager sarà ora possibile configurare Cloud Snapshot Manager come origine degli asset e la vista dashboard mostrerà i dettagli di riepilogo, tra cui le risorse totali protette, non protette, il numero di processi riusciti, i processi non riusciti e così via. Gli utenti possono collegare e avviare Cloud Snapshot Manager per ulteriori dettagli e la gestione dei processi.

Qual è il valore per il cliente di Cloud Snapshot Manager?

Con l'espansione dell'infrastruttura delle aziende nel public cloud, esse si trovano a dover affrontare nuove sfide per proteggere i carichi di lavoro nel cloud. I vantaggi inerenti il cloud, come l'elasticità delle risorse, la facilità di creare nuove macchine virtuali e nuovi database PaaS basati su API, sono altamente desiderati, poiché consentono di ottenere il pieno potenziale dell'IT on demand. Ma hanno bisogno di una soluzione senza agent e che disponga di ricche API di automazione. Inoltre, si trovano a dover proteggere numerose nuove fonti di dati. Devono proteggere le applicazioni tradizionali in esecuzione nella loro infrastruttura cloud e le nuove applicazioni born-in-the-cloud che sfruttano i vantaggi dei servizi PaaS (DBaaS, K8aaS, servizi file). Necessitano di un'ampia serie di API per ottenere l'automazione cloud completa. E la visibilità e il controllo su molti account cloud separati senza necessità di mettere da parte una nuova infrastruttura per ciascun account cloud o di accumulare i costi di trasferimento dei dati inter-VPC/account. Cloud Snapshot Manager risponde a queste sfide.

Ora che Cloud Snapshot Manager può essere attivato con la licenza PowerProtect Data Manager, i clienti non dovranno scegliere tra PowerProtect Data Manager e Cloud Snapshot Manager, o acquistarli separatamente. Ottengono entrambe le soluzioni. In questo modo, è possibile proteggere le applicazioni di livello Enterprise con le potenti funzionalità di PowerProtect Data Manager e APEX Protection Storage, allo stesso tempo avere la possibilità di proteggere migliaia di macchine virtuali e altri database PaaS tramite funzionalità di protezione di Cloud Snapshot Manager basate su tag, senza la necessità di installare agenti o infrastrutture nel cloud.

Come ottenere ulteriori informazioni su Cloud Snapshot Manager?

Accedi a tutte le risorse di vendita e di prodotto pertinenti tramite la pagina SharePoint di PowerProtect Data Manager.

PowerProtect Cyber Recovery

Che cos'è PowerProtect Cyber Recovery?

PowerProtect Cyber Recovery automatizza la creazione e la protezione delle gold copy in un vault dati isolato, garantendo solidi flussi di lavoro di analisi dei dati in un ambiente "clean room".

Crea una copia immutabile dei metadati di PowerProtect Data Manager Data Mover (ad esempio, il catalogo di backup) in un ambiente isolato e ripristina il salvataggio PowerProtect Data Manager in produzione o in un ambiente di ripristino temporaneo isolato.

PowerProtect Cyber Recovery offre la potenza necessaria a un flusso di lavoro automatizzato per aumentare l'infrastruttura di protezione dei dati con un vero isolamento ed esame dei dati, analisi e, cosa più importante, ripristino dei dati per una maggiore resilienza aziendale.

PowerProtect Cyber Recovery è concesso in licenza separatamente da PowerProtect Data Manager?

Pur necessitando l'attivazione tramite un codice di licenza separato, Cyber Recovery è una licenza gratuita ordinabile nell’ambito del percorso di ordinazione di PowerProtect Data Manager.

PowerProtect Cyber Recovery fa parte dei diritti inclusi quando si acquista PowerProtect Data Manager.

È possibile accedere a PowerProtect Cyber Recovery da PowerProtect Data Manager?

No, PowerProtect Cyber Recovery è progettato per essere gestito e controllato dall'interno del server di gestione di Cyber Recovery Vault. Nessun reporting o indicazione dell'esistenza di un'istanza di Cyber Recovery viene segnalata all'interno dell'interfaccia di gestione di PowerProtect Data Manager.

Come ottenere ulteriori informazioni su PowerProtect Cyber Recovery?

Accedi a tutte le risorse di vendita e di prodotto pertinenti tramite il sito SharePoint di PowerProtect Cyber Recovery.

Path to PowerProtect

Che cos'è Path to PowerProtect?

Path to PowerProtect è uno strumento che consente ai clienti di effettuare la transizione da Avamar a PowerProtect Data Manager. Lo scopo principale corrente dello strumento è aiutare a integrare le policy di protezione dei dati di Data Manager sfruttando le policy Avamar esistenti.

Quali sono i carichi di lavoro supportati da Path to PowerProtect oggi?

Path to PowerProtect supporta la migrazione di VMware, file system (inclusi Windows e Linux), SQL e policy Oracle. Lo strumento supporterà la creazione di nuove policy di PowerProtect Data Manager in base alla policy Avamar esistente OPPURE alla possibilità di assegnare gli asset in una policy Avamar a una policy di Data Manager esistente.

Quali carichi di lavoro sono pianificati?

Path to PowerProtect prevede di supportare AIX quest'anno e NDPM in futuro.

Path to PowerProtect supporta attualmente l'appliance PowerProtect Data Manager (DM5500)?

Il supporto per DM5500 sarà ufficialmente disponibile nella prossima release, 1.0.6, prevista per il 19/6/23. Qualsiasi cliente che necessiti del supporto di DM5500 come destinazione di migrazione può ottenerlo tramite una richiesta RPQ.

Path to PowerProtect è disponibile per i clienti?

Path to PowerProtect è oggi disponibile per i clienti Data Manager tramite i servizi.

Qual è il costo di questo strumento?

Lo strumento è disponibile per i clienti con PowerProtect Data Manager gratuitamente, che ne hanno diritto come parte della licenza di PowerProtect Data Manager.

Come posso accedere allo strumento Path to PowerProtect oggi stesso?

Lo strumento è un OVA standalone che può essere richiesto ai servizi. I servizi possono fornire il download dello strumento ai clienti e possono aiutare con l'installazione dello strumento. Una volta completata la migrazione, i servizi possono aiutare anche per la disinstallazione dello strumento.

Lo strumento sarà disponibile direttamente ai clienti?

Sì, il piano è quello di fornire una versione disponibile su larga scala che i clienti possono installare e utilizzare. TUTTI i clienti con Data Manager avranno diritto allo strumento.

Perché Path to PowerProtect è uno strumento separato e non è integrato in PowerProtect Data Manager?

Lo strumento Path to PowerProtect è attualmente uno strumento separato, in modo da poter rispondere alle richieste dei clienti e consentire interruzioni incrementali delle funzionalità. Lo strumento ha lo scopo di aiutare con la migrazione e, essendo separato da Data Manager, siamo in grado di inviare gli aggiornamenti più velocemente senza richiedere modifiche a Data Manager. Il piano è quello di unire lo strumento con Data Manager come strumento di migrazione integrato una volta supportati i carichi di lavoro core e una volta risolta la maggior parte delle richieste di funzionalità dei clienti.

E per quanto riguarda la migrazione dei dati e la possibilità per i clienti di ritirare i sistemi Avamar?

Stiamo pianificando una funzionalità per permettere ai clienti di poter ritirare i loro sistemi Avamar. Affinché i clienti possano ritirare i propri sistemi Avamar, sarà necessario migrare il catalogo corrente di copie a un altro sistema Avamar. Forniremo ai clienti un modo per eseguire la migrazione dei loro attuali sistemi Avamar in una singola istanza AVE che gestirà le copie LTR su PowerProtect Data Domain. Le copie saranno disponibili per il ripristino e la generazione di report di audit.

In che modo Path to PowerProtect sarà in grado di aiutare i clienti a ritirare i sistemi Avamar?

La possibilità di consolidare i sistemi Avamar del cliente a supporto del ritiro è prevista per la fine dell'anno solare 2023.

Dove posso trovare ulteriori informazioni su Path to PowerProtect?

Di seguito sono riportati i link a demo, laboratori, guide di amministrazione e note di rilascio che delineano le funzioni principali dello strumento:

Demo interattive:

- Path to PowerProtect - Migrazione delle policy delle VM
- Migrazione delle policy SQL di Path to PowerProtect

Laboratori pratici:

- Guida a Path to PowerProtect - HOL0419-02

Presentazioni tecniche interne:

- Guida per amministratori
- Note di rilascio
- Guida al deployment

Note di rilascio:

- Note di rilascio di Dell Path to PowerProtect

Architettura moderna basata su servizi

Quale valore offre ai clienti una moderna architettura basata sui servizi?

Man mano che l'ambiente del cliente continua a trasformarsi, PowerProtect Data Manager supporta la possibilità di evolversi rapidamente per soddisfare le esigenze di IT future tramite API per la scalabilità dei servizi.

PowerProtect si dedica a una cadenza di rilascio più frequente che garantisce di assicurare un'innovazione continua, riducendo al minimo l'impatto sull'upgrade.

Supporto alle vendite

Licenze

Sono un dipendente interno Dell e ho bisogno di licenze per scopi di test. cosa fare?

È possibile inviare una SR chiedendo una licenza NFR. Una volta ricevuto il modulo NFR, è necessario compilare le informazioni e seguire le istruzioni sul modulo.

Come viene concessa la licenza di PowerProtect Data Manager?

PowerProtect Data Manager è concesso in licenza da Front End Terabyte (FETB) e dal socket sia in modalità perpetua che in abbonamento. Per ulteriori informazioni, consulta i seguenti manuali per l'ordinazione e la licenza del software per la protezione dei dati:

Guida alle licenze

Un cliente può aggregare la capacità da proteggere di più siti per ottenere l'idoneità per il tier Capacity?

Sì. non ci sono limitazioni sul numero di siti che è possibile installare in PowerProtect Data Manager.

Ordinazione e assistenza

Come posso ordinare PowerProtect Data Manager?

Tutte le versioni di PowerProtect Data Manager possono essere ordinate in DSA/Gii.

Quali sono i limiti di capacità o socket su PowerProtect Data Manager Essentials?

Il limite per PowerProtect Data Manager Essentials è di 50 TB o socket.

Quali sono i servizi di supporto disponibili per PowerProtect Data Manager e quando dovrei consigliarli?

ProSupport Infrastructure Suite risolve i problemi IT in meno tempo e con meno impegno da parte del cliente, spesso rilevandoli prima che si verifichino. Il tipo di servizio di supporto da consigliare dipende dalla complessità dell'ambiente del cliente e dal modo in cui alloca le risorse IT. Le opzioni comprendono:

- **ProSupport Plus**: quando consigli il nostro più alto livello di supporto, i clienti ottengono tutte le funzionalità di ProSupport e un livello più elevato di personalizzazione, tra cui un Service Account Manager assegnato, l'accesso prioritario ai tecnici di assistenza esperti, nonché l'analisi predittiva per la prevenzione dei problemi abilitata dal nostro gateway con connessione sicura. ProSupport Plus include un tempo di risposta mission critical di 4 ore per la sostituzione dei componenti on-site, a seconda del livello di severity.
- **ProSupport**: gli esperti gestiscono la risoluzione dei problemi IT 24 ore su 24, 7 giorni su 7 e risolvono le problematiche hardware o software per i sistemi di data center, disponibili per l'acquisto il giorno lavorativo successivo alla chiamata OPPURE con risposta mission critical entro 4 ore.

ProDeploy Infrastructure Suite aiuta i clienti a trarre il massimo vantaggio dalla loro tecnologia già dal primo giorno. Con PowerProtect Data Manager sono disponibili le seguenti offerte di ProDeploy Infrastructure Suite:

- **ProDeploy Plus**: la scelta migliore per ottimizzare le prestazioni a lungo termine dei sistemi mission-critical con un unico punto di contatto locale per il project management. ProDeploy Plus offre installazione 24x7 e configurazione del software del sistema sempre on-site, 30 giorni di assistenza per la configurazione post-deployment e crediti formativi per Dell Education Services.
- **ProDeploy**: pianificazione, installazione e configurazione da parte di esperti per aiutare i clienti ad adottare rapidamente nuove tecnologie, con un unico punto di contatto per il project management. ProDeploy fornisce pianificazione dell'implementazione, installazione hardware on-site 24x7 e installazione e configurazione 24x7 del software di sistema, oltre alla documentazione di progetto e al trasferimento delle conoscenze.

- **Production Ready for Backup:** una volta eseguito il deployment di Data Manager, il servizio Production Ready for Backup si concentra sulla personalizzazione della tecnologia Data Manager, impiegando tempo per comprendere l'ambiente specifico del cliente e traducendo le sue esigenze specifiche in policy di backup e protezione dei dati. Consigliato per i clienti che hanno requisiti richiesti dalle normative vigenti, problematiche specifiche associate allo SLA o un divario di competenze in ambito di protezione dei dati. Può essere venduto con ProDeploy/ProDeploy Plus o standalone.
- **Deployment Add-on**: Dell offre servizi specializzati per aggiungere scalabilità o funzionalità al di fuori dell'ambito standardizzato di ProDeploy, ProDeploy Plus e Production Ready. Sono utilizzati per implementare le funzionalità specificate disponibili con Data Manager senza pagare per i servizi di cui il cliente non ha bisogno, il tutto è ordinabile con semplici SKU add-on. Disponibile nel punto vendita o in seguito.
- **Additional Deployment Time**: un servizio con ambito flessibile standard per segmenti di tempo di 4 ore da remoto o 8 ore on-site, fornito da un esperto certificato Dell. Utilizzarlo per integrare ProDeploy Infrastructure Suite in modo da soddisfare esigenze aggiuntive o non incluse nell'ambito, ora o fino a 1 anno dopo l'acquisto. Semplifica la distribuzione e riduce al minimo la necessità di Descrizioni del servizio personalizzate.

  È possibile utilizzare Additional Deployment Time per una serie di attività, ad esempio:

- Ambito esteso: requisiti aggiuntivi oltre alle offerte standard
- Esigenze impreviste: assistenza imprevista in qualsiasi momento entro il primo anno
- Attività ad hoc: esigenze a breve termine senza lo sforzo di un processo di preventivo personalizzato.
- **Servizi Data Migration:** i servizi Data Migration aiutano a spostare i dati in modo efficiente, agevolando la transizione ai nuovi prodotti Dell Data Protection e alleggerendo il carico per IT e amministratori. Ideale per i clienti che stanno eseguendo il refresh a nuove tecnologie di storage, consolidano i dati distribuiti o hanno preoccupazioni o problemi precedenti con l'esecuzione tempestiva delle migrazioni per un'iniziativa più ampia.
- **Servizi di residenza**: ideali per i clienti PowerProtect con una base installata di grandi dimensioni o ambienti complessi, i servizi di residenza mettono a disposizione un esperto di protezione dei dati dedicato per colmare il divario di risorse, gestire le operazioni quotidiane e aiutare i team a effettuare la transizione a nuove tecnologie. Disponibili per minimo 1 e 2 settimane.

Come si possono ordinare Professional Services o Formazione per i clienti?

I servizi professionali più comuni sono disponibili per l'ordine negli strumenti di ordinazione Dell. Per ordinare articoli non presenti in elenco, utilizzare i singoli solution path della tecnologia.

Come posso ordinare servizi standard al momento dell'acquisto (POS)?

Per le vendite di nuovi hardware e data manager, i servizi sono disponibili negli strumenti di ordinazione Dell.