

Dell EMC Integrated Data Protection Appliance with PowerProtect Data Manager Best Practices

Abstract

This document discusses best practices for using the Dell EMC™ Integrated Data Protection Appliance (IDPA) with Dell EMC PowerProtect Data Manager. This solution enables efficient and comprehensive data protection for proven and modernized workloads.

July 2020

Revisions

Date	Description
July 2020	Initial release

Acknowledgments

Author: Sandeep Rajagopal

The information in this publication is provided “as is.” Dell Inc. makes no representations or warranties of any kind with respect to the information in this publication, and specifically disclaims implied warranties of merchantability or fitness for a particular purpose.

Use, copying, and distribution of any software described in this publication requires an applicable software license.

Copyright © 2020 Dell Inc. or its subsidiaries. All Rights Reserved. Dell Technologies, Dell, EMC, Dell EMC and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be trademarks of their respective owners. [7/29/2020] [Best Practices] [H18448]

Table of contents

Revisions.....	2
Acknowledgments.....	2
Table of contents	3
Executive summary.....	4
1 Introduction.....	5
1.1 Integrated Data Protection Appliance.....	5
1.1 PowerProtect Data Manager	5
2 PowerProtect Data Manager with IDPA overview.....	7
2.1 Example use case: Protecting Kubernetes workloads	7
2.2 Key benefits	8
3 Technical considerations and deployment	9
3.1 Prerequisites.....	9
3.2 PowerProtect Data Manager deployment	9
3.3 Data Protection Central deployment.....	10
3.3.1 Disabling Integrated Data Protection Appliance System Manager	10
3.3.2 Registering IDPA and PowerProtect Data Manager to an external instance of Data Protection Central	12
3.4 Discovering the embedded Data Domain system with PowerProtect Data Manager	15
4 Interoperability and limits.....	18
5 Summary	19
A Technical support and resources	20
A.1 Related resources	20

Executive summary

Data protection is an integral and essential part of any successful business. Organizations and IT teams require a proven, powerful, modern, scalable, and easy-to-use data protection solution.

To meet market demands, Dell Technologies™ offers a unique solution consisting of Dell EMC™ PowerProtect Data Manager with Dell EMC Integrated Data Protection Appliance (IDPA). The IDPA protects leading enterprise applications and operating systems. The PowerProtect Data Manager solution protects traditional workloads such as file system, SQL, SAP® HANA®, Oracle®, and Microsoft® Exchange. It also protects modern, cloud-native Kubernetes workloads and enables differentiated VMware® protection.

Integrating the proven IDPA with the modern PowerProtect Data Manager enables you to get the most efficient and comprehensive data protection solution for your modernized workloads. Also, you can use the Dell EMC Data Domain™ system that is bundled with IDPA as back-end storage for PowerProtect Data Manager workloads at no extra cost.

Audience

The information in this document is intended for customers who are responsible for planning, implementing, and administering the environments that contain IDPA solutions. The primary audience consists of customers, customer service, and remote Professional Services engineers.

1 Introduction

This section provides an overview of the Integrated Data Protection Appliance and PowerProtect Data Manager software.

1.1 Integrated Data Protection Appliance

The Integrated Data Protection Appliance (IDPA) is an all-in-one backup appliance that reduces the complexity of managing multiple data silos, point solutions, and vendor relationships. IDPA simplifies deployment and management while delivering powerful, enterprise-grade data protection capabilities for small, midsized, and enterprise organizations with a low cost-to-protect ratio.

The IDPA provides a solution for data-protection administrators who are accustomed to configuring and managing one or more data-protection and storage devices, but are challenged to manage independent and disconnected applications.

IDPA System Manager enables administrators to efficiently manage the IDPA components from a single user interface. This interface includes monitoring, reporting, analytics, and search capabilities to help simplify the data-protection experience.

The IDPA (Figure 1) streamlines the configuration and the integration of data-protection components in a consolidated solution and also offers the following benefits:

- Simplified deployment and configuration
- Backup administration
- Deduplication
- Native cloud data reduction (DR) and long-term retention (LTR)
- Instant access and restore
- Monitoring and analytics
- Search
- Scalability
- Unified support



Figure 1 Dell EMC Integrated Data Protection Appliance

1.1 PowerProtect Data Manager

Dell EMC PowerProtect Data Manager software is an enterprise solution that provides software-defined data protection, deduplication, operational agility, self-service, and IT governance.

PowerProtect Data Manager enables the transformation from traditional centralized protection to an IT-as-a-service model that is based on a self-service design. This design ensures that you can enforce compliance and other business rules, even when backup responsibilities are decentralized to individual database administrators and application administrators.

PowerProtect Data Manager (shown in Figure 2) supports multiple workloads such as the following:

- Kubernetes
- Filesystem
- Databases
- Virtual machines
- Storage-Direct (SDM)

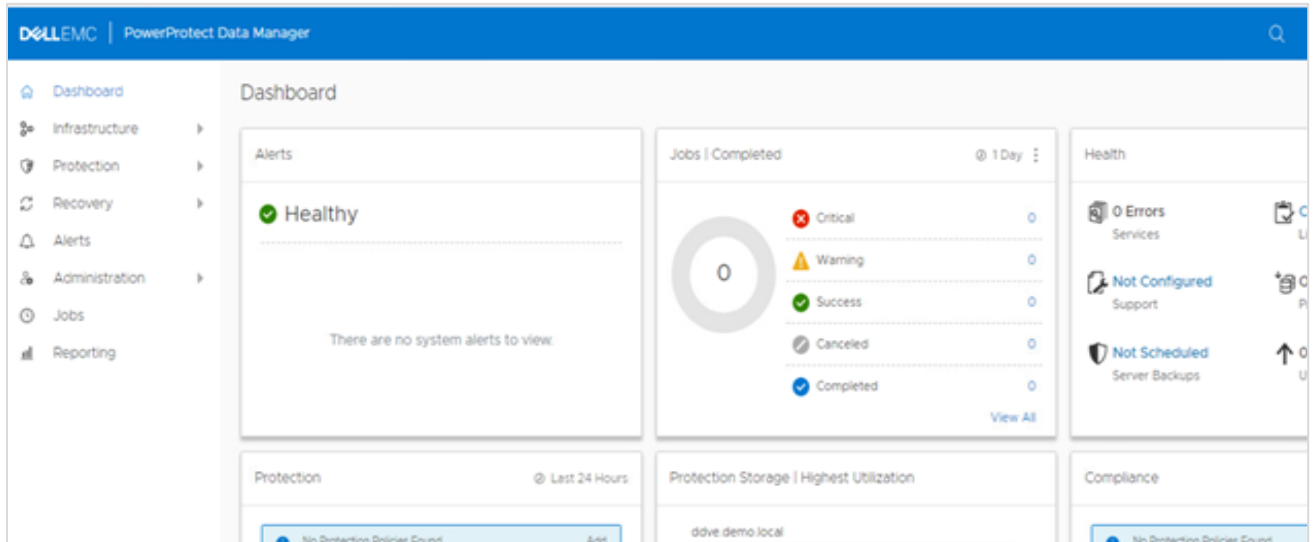


Figure 2 PowerProtect Data Manager

2 PowerProtect Data Manager with IDPA overview

The IDPA protects leading enterprise applications and operating systems. The PowerProtect Data Manager solution protects traditional workloads such as file system, SQL, SAP® HANA®, Oracle®, and Microsoft® Exchange. It also protects modern, cloud-native Kubernetes workloads and offers differentiated VMware® protection.

Integrating the proven IDPA with modern PowerProtect Data Manager enables you to get the most efficient and comprehensive data protection solution for your modernized workloads. Also, you can use the Dell EMC Data Domain™ system that is bundled with IDPA as back-end storage for PowerProtect Data Manager workloads at no extra cost.

PowerProtect Data Manager delivers a simplified user interface that is easy to navigate. It eases the process and reduces the number steps required for creating backups, replication, recovery, expansion, and upgrades. Monitoring, managing, and analyzing copies of data are no longer tedious tasks with PowerProtect Data Manager, which also addresses the issue of copy sprawling.

PowerProtect Data Manager provides centralized governance that helps mitigate risk and assures compliance of service-level agreements (SLAs) and service-level objectives (SLOs) through simple protection workflows.

PowerProtect Data Manager enables automated discovery and onboarding of the following:

- Databases
- Virtual machines
- Kubernetes clusters
- Data Domain protection storage

It also offers self-service and centralized protection for Microsoft® SQL Server®, Microsoft Exchange, SAP HANA, and Oracle databases, and is multicloud optimized for efficient, long-term retention and disaster recovery.

When you use the embedded Data Domain in IDPA as the target storage for unique workloads, you get secondary storage with unmatched efficiency, deduplication, performance, and scalability at no extra cost. This result combines the best of proven and modern data protection solutions.

2.1 Example use case: Protecting Kubernetes workloads

Today, containers have increased in popularity. Containers are like virtual machines but have relaxed isolation properties to share the operating system. This container has its own file system, CPU, memory, and process space. Key benefits of containers include agile application creation, continuous development, environmental consistency across development, application-centric management, efficient resource allocation, and resource isolation.

With distributed container deployment, it is necessary to protect the workloads. PowerProtect Data Manager allows protecting the production workloads in Kubernetes (K8s) environments. This capability ensures the data is easy to back up and restore, always available, consistent, and durable in a Kubernetes workload or DR situation.

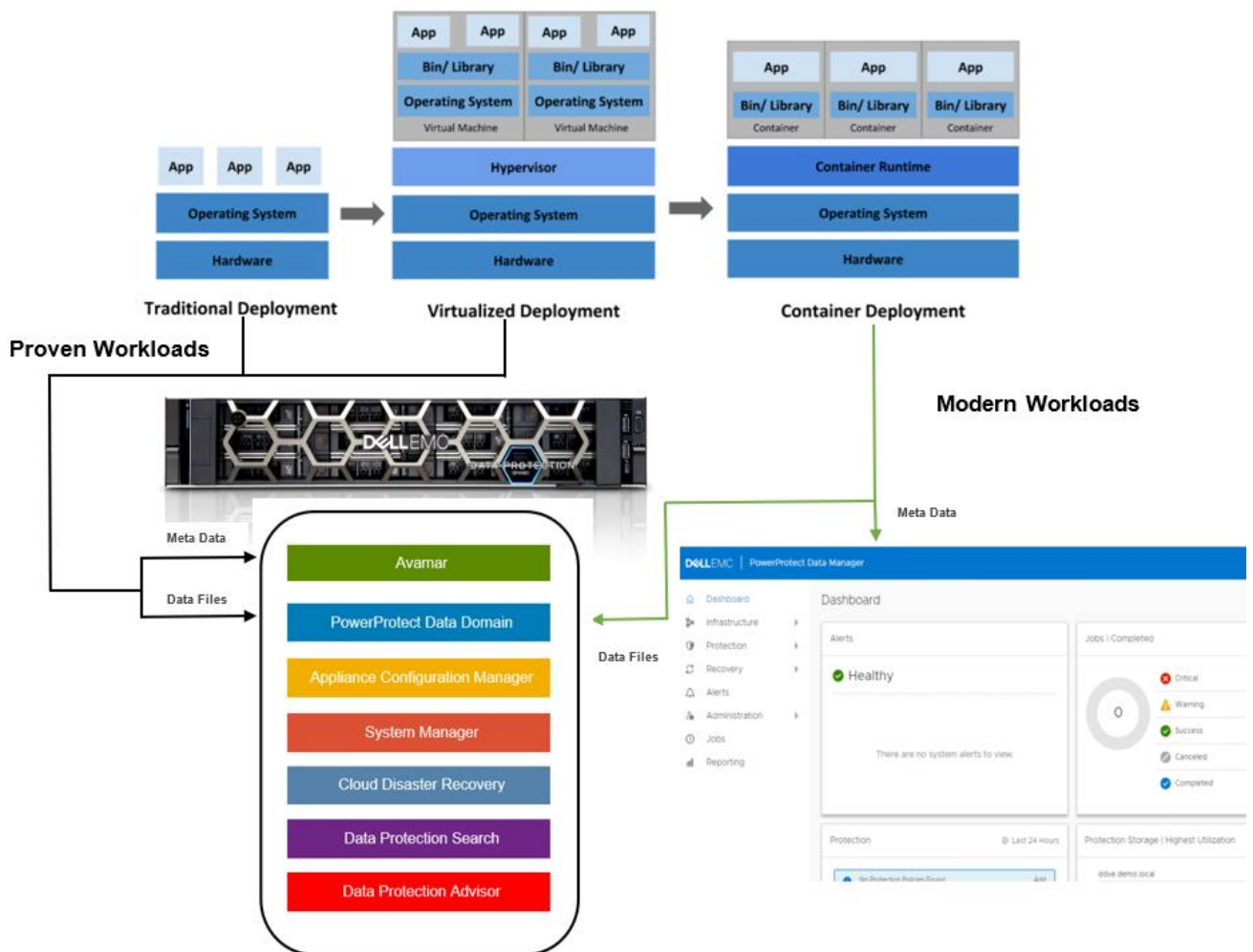


Figure 3 PowerProtect Data Manager with IDPA

2.2 Key benefits

With IDPA protecting leading enterprise applications, virtual machines, and operating systems, and with PowerProtect Data Manager protecting modern workloads such as Kubernetes, you have an efficient and optimized data-protection solution.

For modern workloads, you are protected with embedded Data Domain systems, and can have secondary storage with unmatched efficiency, deduplication, performance, and scalability at no extra cost.

For more information about configuring PowerProtect Data Manager, see the [PowerProtect Data Manager Administration and User Guide](#).

3 Technical considerations and deployment

This section provides prerequisites, best practices, and deployment guidance for using IDPA with PowerProtect Data Manager.

3.1 Prerequisites

Ensure that Dell EMC IDPA is deployed, configured, and operating.

3.2 PowerProtect Data Manager deployment

It is vital to plan for the environment that is used for deploying PowerProtect Data Manager, and to facilitate adequate resources to achieve optimal performance of PowerProtect Data Manager.

The PowerProtect Data Manager software appliance is easy to install and configure. You can deploy the PowerProtect Data Manager Open Virtual Appliance (OVA) using one of the following methods:

- Manually deploying the OVA to a VMware vCenter® server: Use this method to deploy the OVA to a stand-alone or cluster host while logged into the vCenter server. This method allows you to configure the network settings during deployment.
- Manually deploying the OVA to a VMware ESXi™ host: Use this method to deploy the OVA while logged in to an ESXi host. Use the VM console to configure the network settings after the deployment completes.

Minimum requirements:

The minimum resource requirements to deploy a PowerProtect Data Manager in vSphere 6.0 and above are as follows:

- 10 CPU cores
- 18 GB RAM
- 700 GB disk space

If you plan to use **Cloud DR**, your system must also meet the following requirements:

- 14 CPU cores
- 22 GB RAM

See section 4 to check for interoperability.

Best practices:

- Deploy the PowerProtect Data Manager Software on an external vCenter Server.
- Create a dedicated PowerProtect vCenter user and avoid using vCenter administrator credentials.
- Create a dedicated PowerProtect Data Domain BOOST User for Data Domain Discovery.

See the *PowerProtect Data Manager Deployment Guide* for more deployment information.

3.3 Data Protection Central deployment

It is critical to plan for the environment that is used to deploy Data Protection Central and provide the appropriate resources to optimize its performance. This section describes how to install and configure Data Protection Central.

Before you begin deployment, review the following information:

- Ensure the network is set up with IDPA and PowerProtect Data Manager is set up.
- Ensure the DNS is set up correctly. The correct DNS setup ensures that systems monitored by Data Protection Central can resolve the Data Protection Central hostname and Fully Qualified Domain Name (FQDN).
- Ensure the time synchronization between the IDPA and PowerProtect Data Manager is correct for efficient and effective monitoring of components.
- Deploy the Data Protection Central Open Virtualization Appliance (OVA) using a VMware vSphere® client.
- Ensure the minimum resource requirements are met to deploy Data Protection Central:
 - 4 CPU cores
 - 8 GB RAM
 - 550 GB disk space

Note: The Data Protection Central OVA does not deploy directly on an ESXi server.

- For optimal performance, you must deploy the external Data Protection Central component outside the IDPA vCenter for optimal performance.
- See section 4 to check for interoperability.

For more information, see the *Data Protection Central Getting Started Guide*.

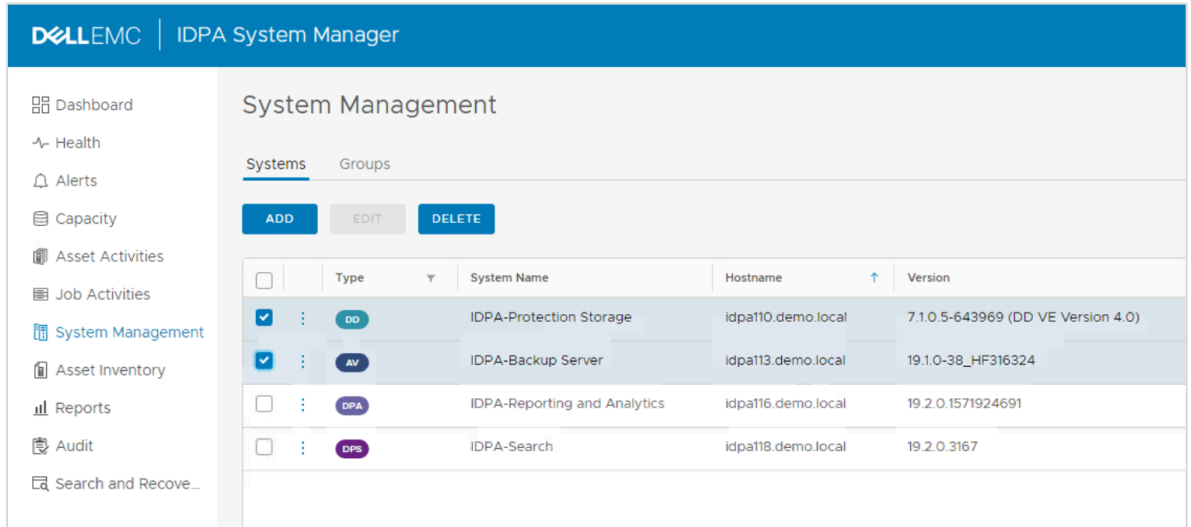
3.3.1 Disabling Integrated Data Protection Appliance System Manager

IDPA System Manager enables administrators to efficiently monitor and manage the software products within the IDPA from a single user interface, simplifying the data-protection experience.

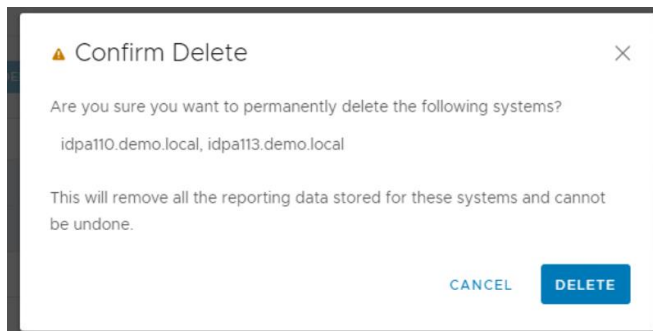
With PowerProtect Data Manager and IDPA, you cannot use the embedded system manager to efficiently monitor the PowerProtect Data Manager activities. To efficiently monitor both IDPA and PowerProtect Data Manager, you must deploy an external instance of Data Protection Central.

To unregister the IDPA backup server and IDPA protection storage components from the embedded system manager, perform the following steps.

1. Log in to **IDPA System Manager**.
2. In the left menu, click **System Management**.
3. Select **IDPA-Backup Server** and **IDPA-Protection Storage**.



4. Click **Delete**. The **Confirm Delete** window appears.



5. Click **Delete**.

The system is removed. A deactivation activity message appears on the **Audit** page.

Note: Follow the above procedure to unregister Data Protection Advisor and Data Protection Search from the embedded System Manager.

3.3.2 Registering IDPA and PowerProtect Data Manager to an external instance of Data Protection Central

With PowerProtect Data Manager and IDPA, it can be cumbersome to manage and monitor the activities of a proven and modern data-protection solution individually.

Deploying an external Data Protection Central component enables administrators to efficiently monitor and manage both IDPA and PowerProtect Data Manager from a single user interface. This ability simplifies the entire data protection experience for the customer.

Also, registering external Data Protection Advisor and Data Protection Search components with Data Protection Central enables common reporting and search capabilities for both IDPA and PowerProtect Data Manager.

Note: Only one external Data Protection Advisor and Data Protection Search component can be configured with an external instance of Data Protection Central.

The minimum software requirements to complete this process are as follows:

- PowerProtect Data Manager 19.5
- Data Protection Central 19.3
- Data Protection Advisor 19.3 (external)
- Data Protection Search 18.2/19.1/19.2/19.3 (depending on IDPA models)

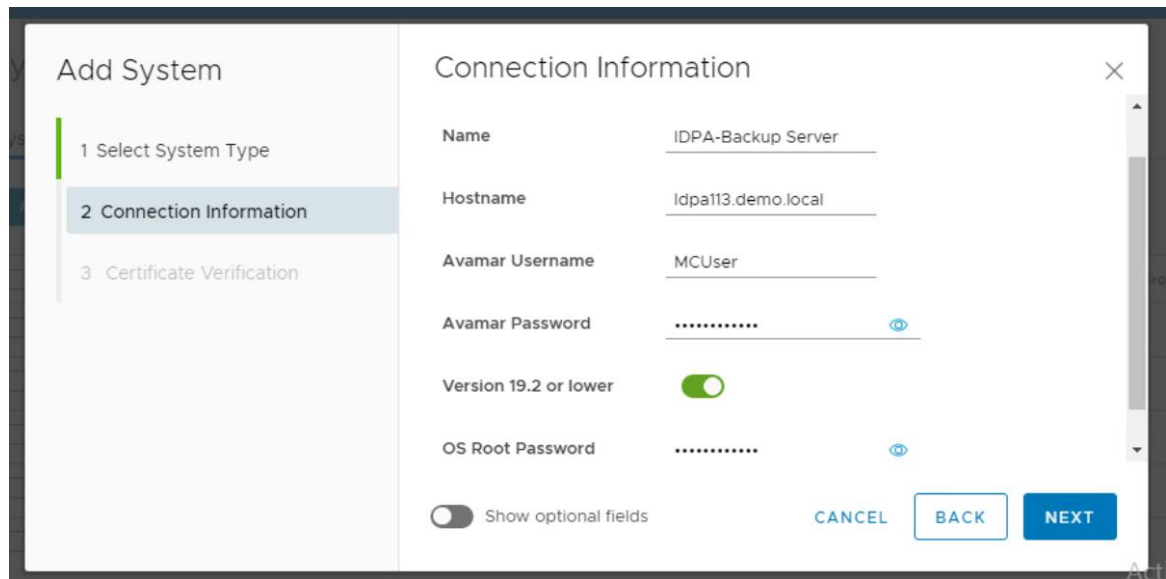
This process assumes that an external Data Protection Central instance has been deployed.

Adding an IDPA backup server:

1. Log in into Data Protection Central.
2. In the left menu, click **System Management**.
3. Click **Add**. The **Add System** window is displayed.
4. On the **Select System Type** page, select **Avamar**, and click **Next**.

5. On the **Connection Information** page, specify the following information:
 - **Name:** Specify a name to identify the system.
 - **Hostname:** Specify the FQDN of the Avamar system.
 - **Avamar Username:** Specify the username of the Avamar system. For the Avamar administrator, the username is **MCUser**.
 - **Avamar Password:** Specify the password for the Avamar system user interface.

Note: Operating-system root credentials are optional for Avamar 19.3 and later. If the **Avamar version is 19.2 or earlier**, click the **toggle button** to enable the field and specify the **OS root > password**.



The screenshot shows a window titled "Add System" with a sidebar on the left containing three steps: "1 Select System Type", "2 Connection Information" (which is selected and highlighted), and "3 Certificate Verification". The main area is titled "Connection Information" and contains the following fields and controls:

- Name:** IDPA-Backup Server
- Hostname:** Idpa113.demo.local
- Avamar Username:** MCUser
- Avamar Password:** Masked with dots, with a toggle icon to the right.
- Version 19.2 or lower:** A green toggle switch is turned on.
- OS Root Password:** Masked with dots, with a toggle icon to the right.
- Show optional fields:** A toggle switch is turned off.

At the bottom right, there are three buttons: "CANCEL" (light blue), "BACK" (white with blue border), and "NEXT" (blue).

6. Click **Next**.
7. Select the **Accept Certificate** option and click **Save**.

Note: Allow 15 minutes for the data to be synchronized between the Data Protection Central and IDPA backup server.

Adding IDPA protection storage:

1. Log in into Data Protection Central.
2. In the left menu, click **System Management**.
3. Click **Add**. The **Add System** window is displayed.
4. On the **Select System Type** page, select **Data Domain**, and click **Next**.

5. On the **Connection Information** page, specify the following information:
 - **Name:** Specify a name that identifies the system.
 - **Hostname:** Specify the FQDN of the Data Domain system.
 - **Username:** Specify the Data Domain administrator username.
 - **Password:** Specify the Data Domain administrator password.

The screenshot shows a dialog box titled "Add System" with a close button (X) in the top right corner. On the left side, there is a vertical progress bar with three steps: "1 Select System Type", "2 Connection Information" (which is highlighted in blue), and "3 Certificate Verification". The main area of the dialog is titled "Connection Information" and contains the following fields:

Type	Data Domain
Name	IDPA-Protection Storage
Hostname	Idpa110.demo.local
Username	sysadmin
Password

At the bottom right of the dialog, there are three buttons: "CANCEL", "BACK", and "NEXT".

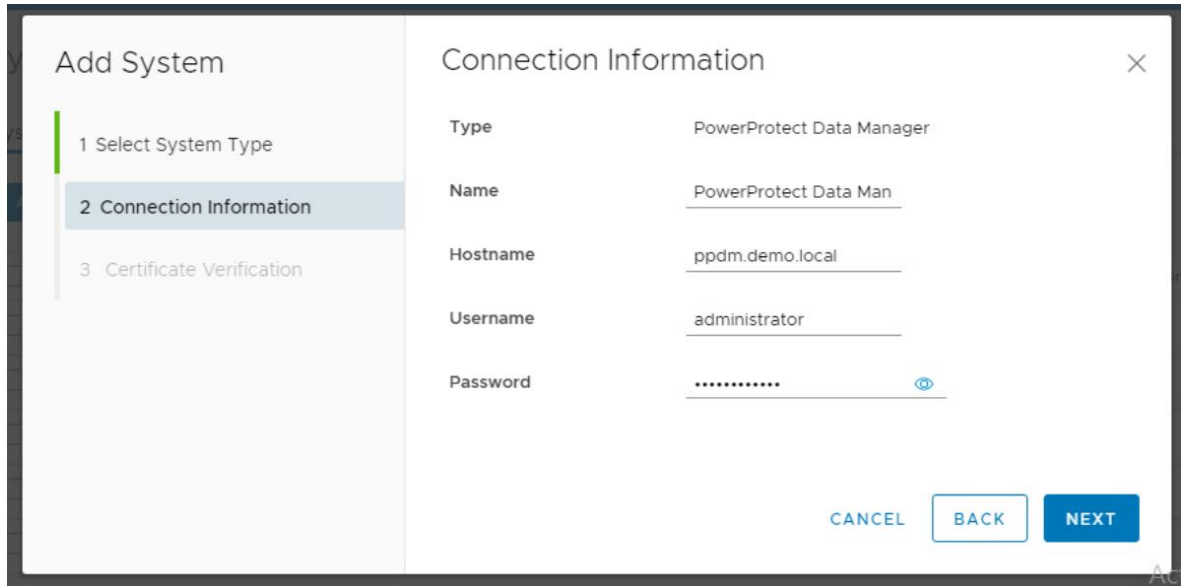
6. Click **Next**.
7. Select the **Accept Certificate** option and click **Save**.

Note: Allow 15 minutes for the data to be synchronized between the Data Protection Central and IDPA protection storage.

Adding PowerProtect Data Manager:

1. Log in into Data Protection Central.
2. In the left menu, click **System Management**.
3. Click **Add**. The **Add System** window is displayed.
4. On the **Select System Type** page, select **PowerProtect Data Manager**, and click **Next**.

5. On the **Connection Information** page, specify the following information:
 - **Name:** Specify a name that identifies the system.
 - **Hostname:** Specify the FQDN of the PowerProtect system.
 - **Username:** Specify the PowerProtect administrator username.
 - **Password:** Specify the PowerProtect administrator password.



6. Click **Next**.
7. Select the **Accept Certificate** option and click **Save**.

Note: You can also integrate Data Protection Advisor and Data Protection Search to the external Data Protection Central instance using methods similar to the above process.

See the *Data Protection Central Administrator Guide* for more information.

3.4 Discovering the embedded Data Domain system with PowerProtect Data Manager

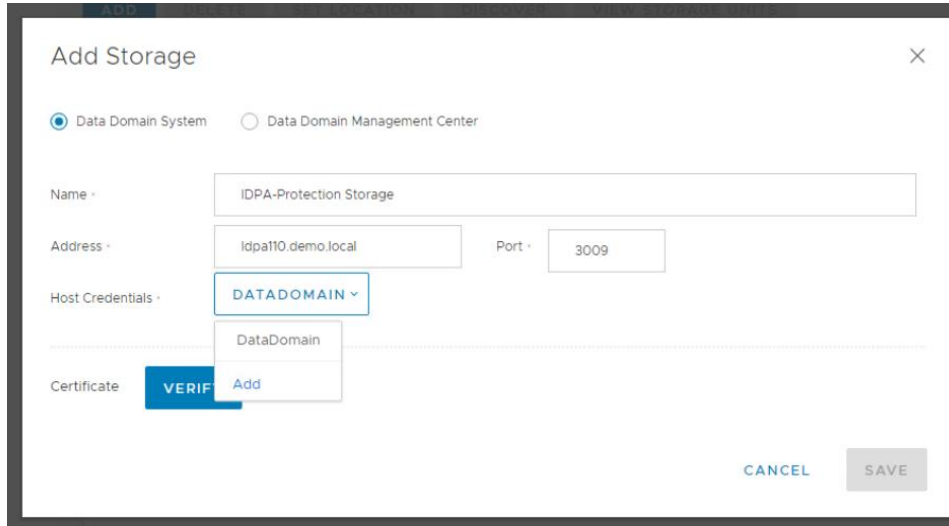
PowerProtect Data Manager leverages the embedded Data Domain in the IDPA as the target server for protecting modern workloads. To start protecting modern workloads, PowerProtect Data Manager must discover the embedded Data Domain system as the target storage server. As a prerequisite, create a dedicated PowerProtect Data Domain Boost User for Data Domain Discovery.

Discovering the embedded Data Domain System:

1. Log in to PowerProtect Data Manager.
2. Click **Infrastructure > Storage**. The **Storage** window appears.
3. In the **Protection Storage** tab, click **Add**.
4. In the **Add Storage** dialog box, select the **Data Domain** system.

5. Specify the **Embedded Data Domain** system attributes:

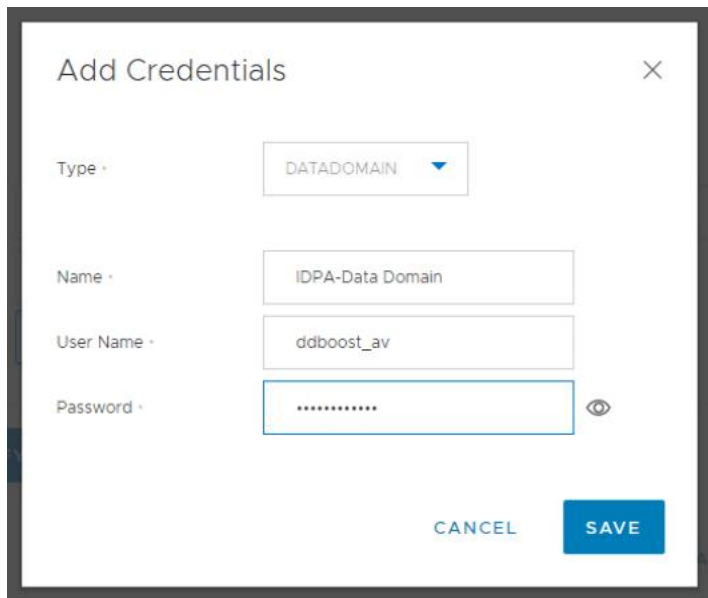
- **Name:** Specify the embedded Data Domain name.
- **Address:** Specify the hostname, FQDN, or the IP address.
- **Port:** Specify the port for SSL communication. The default value is 3009.



6. Under **Host Credentials**, click **Add**.

7. Enter the following information in the **Add Credentials** window.

- **Name:** Provide a descriptive name to the keychain.
- **Username:** Specify the Data Domain Boost Username for the Data Domain Discovery.
- **Password:** Specify the Data Domain Boost Credentials.



8. Click **Save**.

9. Click **Verify** to review the certificate, and click **Accept**.

10. Click **Save** to exit the **Add Storage** window and initiate the discovery for the **embedded Data Domain System**.

A dialog box appears to indicate that the request to add storage has been initiated.

11. In the **Storage** window, click **Discover** to refresh the window with the embedded Data Domain system information.
12. When a discovery completes successfully, the Status column updates to **OK**.

This process has successfully discovered the embedded Data Domain system as the target storage server with PowerProtect Data Manager. You can now start protecting modern workloads in the embedded Data Domain system, benefiting from secondary storage with unmatched efficiency, deduplication, performance, and scalability.

4 Interoperability and limits

The PowerProtect Data Manager with IDPA solution has the following the minimum software requirements:

- PowerProtect Data Manager 19.5
- Data Protection Central 19.3 (external)
- Data Protection Advisor 19.3 (external)
- Data Protection Search 18.2/19.1/19.2/19.3 (depending on IDPA models)

According to the architecture of PowerProtect Data Manager, for each policy, there is a Storage-Unit that is created on the embedded Data Domain system. You must ensure that you do not run out of Storage-Unit space on the embedded Data Domain system.

Figure 4 (from [E-Lab Navigator](#)) shows the maximum number of MTrees that can be created on the embedded Data Domain system and the total number of MTrees that can be active for both read and write operation.

	Internal IDPA Software					External to IDPA		
	DD VE version	DD OS version	Mtree limits Total/Active	AV version	DPS version (can be external)	PPDM version	External DPC version	External DPA version
IDPA 2.3.x								
DP4x	4.0	6.2.0	100/32	18.2	18.2/19.1	19.5	19.3	19.3
DP5x	NA	6.2.0	128/128	18.2	18.2/19.1	19.5	19.3	19.3
DP8x	NA	6.2.0	256/256	18.2	18.2/19.1	19.5	19.3	19.3
IDPA 2.4.x								
DP4x	4.0	6.2.0	100/32	18.2	18.2/19.1	19.5	19.3	19.3
DP5x	NA	6.2.0	128/128	18.2	18.2/19.1	19.5	19.3	19.3
DP8x	NA	6.2.0	256/256	18.2	18.2/19.1	19.5	19.3	19.3
IDPA 2.5								
DP4x	4.0	7.1.0.5	100/32	19.1	19.2	19.5	19.3	19.3
DP5x	NA	7.1.0.5	128/128	19.1	19.2	19.5	19.3	19.3
DP8x	NA	7.1.0.5	256/256	19.1	19.2	19.5	19.3	19.3
IDPA 2.6								
DP4x	5.0	7.2.x	100/32	19.3	19.3	19.5	19.3	19.3
DP5x	NA	7.2.x	128/128	19.3	19.3	19.5	19.3	19.3
DP8x	NA	7.2.x	256/256	19.3	19.3	19.5	19.3	19.3

Figure 4 Interoperability and limits

Note: One MTree is always reserved for the IDPA backup server.

5 Summary

Dell EMC PowerProtect Data Manager with the Dell EMC IDPA backup appliance provides the benefits of both proven and modern data-protection solutions for modernized workloads. With protection for unique workloads in the embedded Data Domain systems, you can also benefit from secondary storage with unmatched efficiency, deduplication, performance, and scalability at no extra cost.

Also, the external Data Protection Central component enables administrators to efficiently monitor and manage both the IDPA and PowerProtect Data Manager from a single user interface, simplifying the entire data protection experience.

A Technical support and resources

[Dell.com/support](https://www.dell.com/support) is focused on meeting customer needs with proven services and support.

[Storage technical white papers and videos](#) provide expertise that helps to ensure customer success on Dell EMC storage platforms.

A.1 Related resources

For additional information, see the following resources:

- PowerProtect Data Manager Administrator and User Guide
- PowerProtect Data Manager Deployment Guide
- Data Protection Central Getting Started Guide
- Data Protection Central Administrator Guide
- [E-Lab Navigator](#): Provides compatibility information, including specific software and hardware configurations that the solution supports.