DELL Technologies

Technical Whitepaper

Dell EMC Integrated Data Protection Appliance (IDPA) protecting VMware workloads

Abstract

This whitepaper discusses the concept of Dell EMC Integrated Data Protection Appliance (IDPA) and how it protects VMware workloads. This solution enables efficient and comprehensive data protection for proven and modernized VMware workloads.

January 2021

H18630

Revisions

Date	Description
January 2021	Initial release

Acknowledgements

Author: Abhishek Shukla, Solutions Technical Marketing Team, Data Protection Domain

Table of contents

Revisions 2
Acknowledgements 2
Table of contents 3
Executive summary 4
Audience 4
Scope 4
1 Introduction 5
1.1 Components of IDPA 5
1.1.1 Appliance Configuration Manager (ACM) 5
1.1.2 Dell EMC Avamar 5
1.1.3 IDPA System Manager 6
1.1.4 PowerProtect Data Domain (PowerProtect DD) 6
1.1.5 Data Protection Search (DPS) 6
1.1.6 Cloud Disaster Recovery Appliance (CDRA) 6
1.1.7 Data Protection Advisor (DPA) 6
2 Deployment 7
2.1.1 ACM Setup 7
2.1.2 Components Setup 8
3 Protecting VMware Workloads 10
3.1 Navigating to Avamar UI 10
3.2 Register vCenter with IDPA 10
3.3 Add Virtual Machine as Client to be protected 12
3.4 Proxy Deployment 12
3.5 Add Dataset 13
3.6 Backup 14
3.7 Restore 15
A Technical support and resources 16
A.1 Related resources 16

Executive summary

In the modern era of technology, Data is important that visualizes the strength of a business and Data Protection is one of the most important aspect and challenge for the successful business. Organizations are leveraging virtualized environment for their workloads and require a proven, modern, scalable, reliable and easy-to-use data protection solution to protect modernized workloads.

To meet these demands, Dell Technologies offers a unique platform called Integrated Data Protection Appliance (IDPA) which provides converged solution including backup and recovery with replication, instant access, search and analytics, reporting with deduplication and cloud integration, disaster recovery and long-term retention.

The IDPA provides a simplified configuration and the integration of data protection components in a consolidated solution. It is configured to protect itself from data loss with the backup and storage application included in the system

Audience

This document is intended for anyone 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

Scope

The scope of this whitepaper is limited to the DP4400 version which is hyper-converged solution of IDPA and provides the virtual environment with Avamar Virtual Edition (AVE) as the Backup node, Data Domain virtual Edition (DDVE) as the Protection Storage node

IDPA version 2.6

1 Introduction

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 configure and manage 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 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

1.1 Components of IDPA

IDPA is called Integrated solution for data protection as it combines multiple data protection solutions into a single product.

1.1.1 Appliance Configuration Manager (ACM)

Application Configuration Manager is the component which enables the configuration of IDPA by providing a web-based interface for configuration, upgrade and monitoring appliance. It also allows to modify configuration details i.e. expanding the Data Domain disk capacity, change the common password for the appliance, change LDAP settings, update customer information, and change the values in the General Settings panel.

1.1.2 Dell EMC Avamar

IDPA uses Dell EMC Avamar as backup solution for the workloads. Dell EMC Avamar is proven backup and recovery software that delivers secure data protection for cloud, remote office and data centers. It has tight integration with VMware interfaces which makes it a great solution for protecting any workloads running in a virtualized environment. Avamar has two flavors i.e. Physical Avamar and Avamar Virtual Edition (AVE). IPDA uses AVE servers for DP400 and DP5xxx series models and

physical Avamar for DP8xxx series models to perform backup operations. Optionally, Network Data Management protocol (NDMP) accelerator can be added to enable backup and recovery of NAS systems.

1.1.3 IDPA System Manager

The IDPA System Manager provides the advanced monitoring and management of IDPA activities i.e. backup and recovery, replication, asset management, capacity, health and alerts. It also includes advanced features like search and recover options, comprehensive reporting and cloud backups. The UI has information about Avamar, Data Domain, Search and Data Protection Advisor components.

1.1.4 PowerProtect Data Domain (PowerProtect DD)

PowerProtect DD is an inline deduplication storage system which performs target-based backups, archives and disaster recovery that utilizes high speed processing. The backups performed by Avamar systems are stored in PowerProtect DD, known as protection storage. Like Avamar, the accelerator performs NDMP processing and sends the data directly to PowerProtect DD Server. PowerProtect DD has two flavors i.e. physical server and virtual edition.

1.1.5 Data Protection Search (DPS)

DPS provides a powerful way to search backup data within the IDPA and then restore the backup data based on the results of the search. Scheduled collection activities are used to gather and index the metadata (such as keyword, name, type, location, size, and backup server/client, or indexed content) of the backup, which is then stored within the IDPA.

1.1.6 Cloud Disaster Recovery Appliance (CDRA)

Disaster recovery is one of the important aspects and feature of a data protection solution. CDRA is a solution that enables DR feature of one or more on-premise virtual machines (VMs) to the cloud. It integrates with the existing on-premise backup software and PowerProtect DD to copy the VM backups to the cloud. It then runs a disaster recovery test or a failover, which converts a VM to an AWS EC2 instance, and runs this instance in the cloud.

1.1.7 Data Protection Advisor (DPA)

DPA provides reporting and analytics that offers a reporting functionality with dedicated sections for various features. The reports help to retrieve information about the Protection Storage and Avamar (AVE). Using these reports, outages can be easily identified in the environment, diagnose problems, plan to mitigate risks, and forecast future trends.

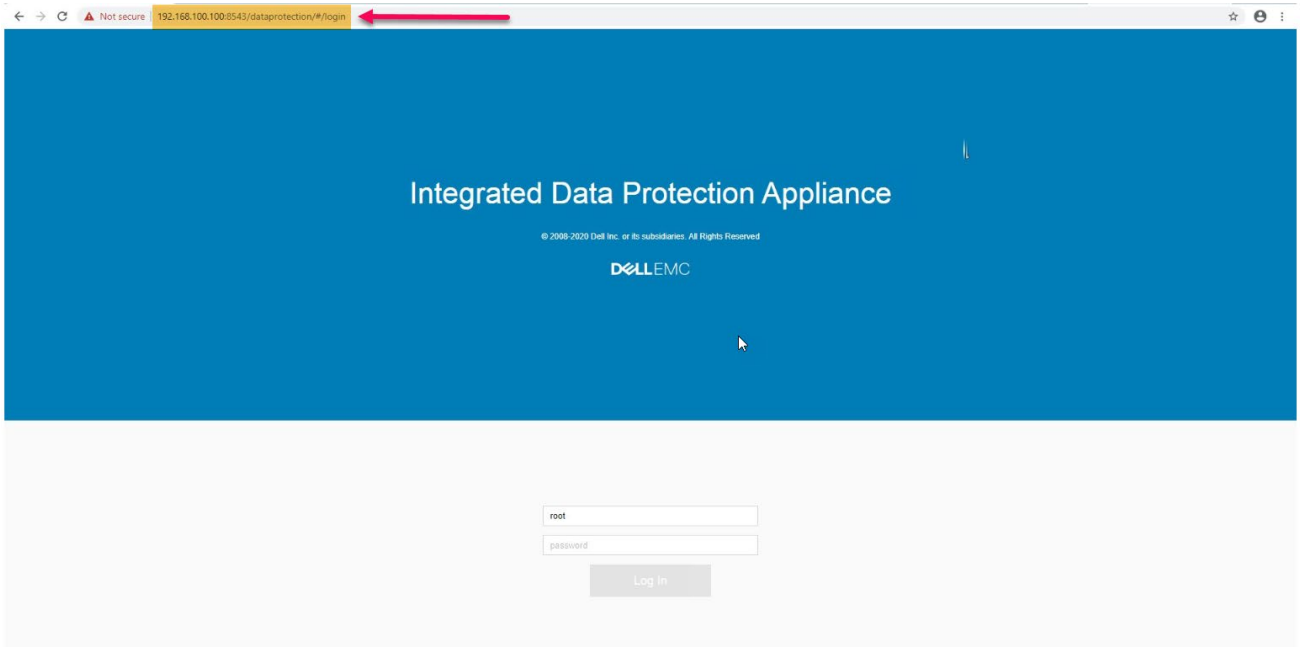
Note: Components like CDRA, DPS or DPA are optional. Also, if these components are already configured in environment, then the appliance can be configured to use the central implementation

2 Deployment

IDPA DP4400 is a converged virtual appliance. It is fully integrated with components of IDPA models into single 2U node and is faster to deploy.

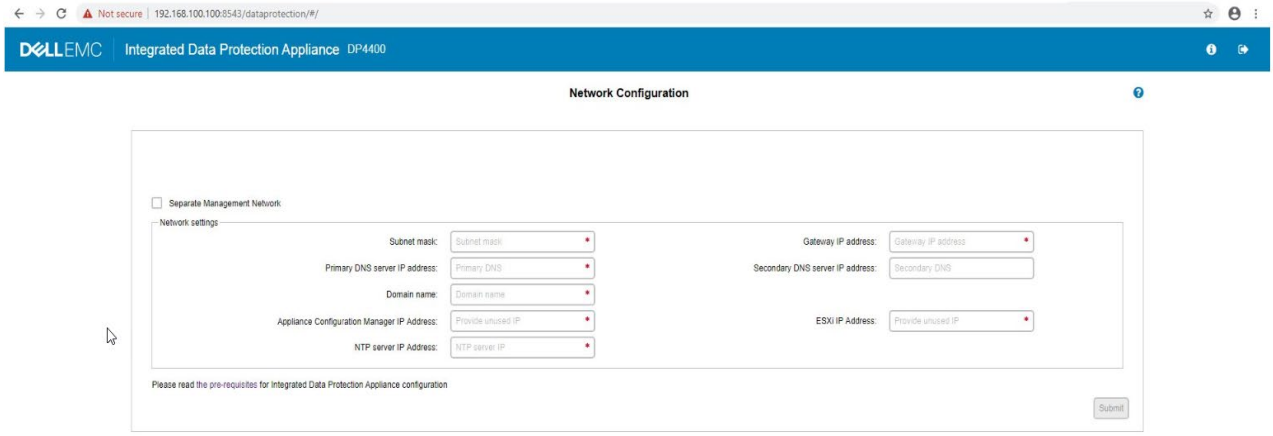
2.1.1 ACM Setup

ACM is the component that deploys IDPA. ACM set up is one-time process and configured initially. When IDPA is shipped, it is accessible with default IP address https://192.168.100.100:8543 using default 'root' credentials.

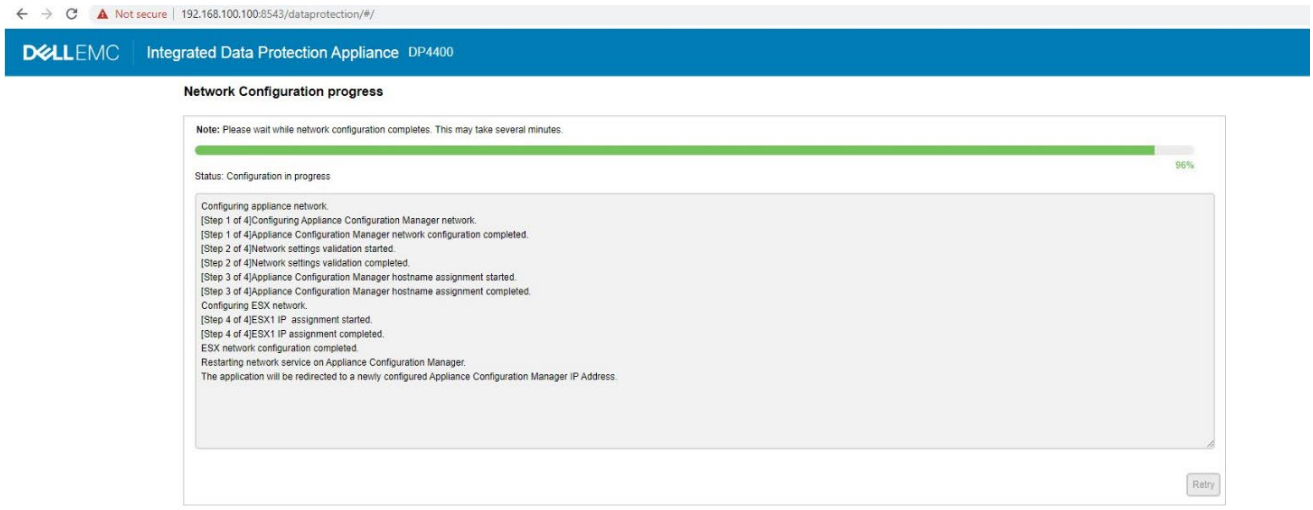


Landing page when IDPA is connected with default IP address

When the default username and password are entered, it prompts to change the password. Also, this page allows to configure with the network details that includes IP address of ACM (customer's



network), subnet mask, DNS and IP address of ESXi host.



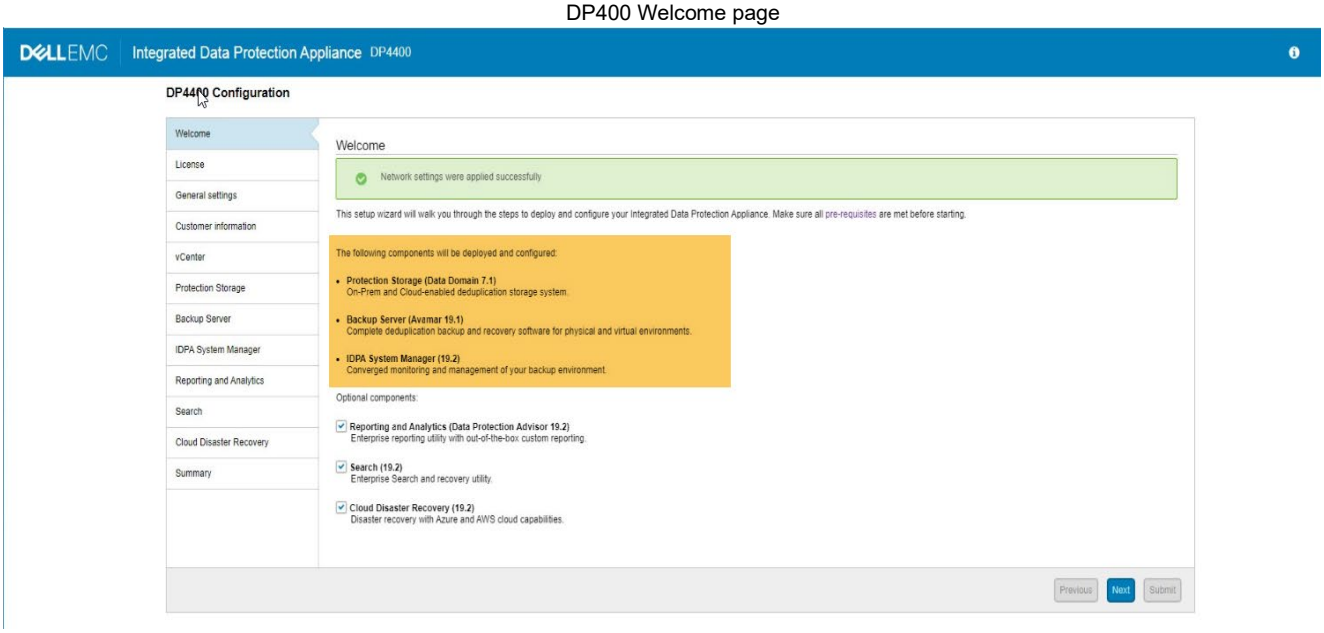
Network Configuration Set up

It takes several minutes to complete the network configuration, Once completes, ACM set up is done. The login credential is the new IP address (set for ACM IP) with new password you set for "root".

2.1.2 Components Setup

ACM is responsible to deploy the IDPA appliance and the components. Once logged-in with root credentials, DP400 Configuration page tells about the components to be configured.

DP400 Welcome page



Mandatory Components

- Protection Storage (PowerProtect Data Domain)
- Backup Server (Avamar)
- IDPA system manager

Optional Components

- Reporting and Analytics (DPA)
- Search (DPS)
- Cloud Disaster Recovery (CDRA)

Note: Each component i.e. Protection Storage (Data Domain), Backup server (Avamar) and Reporting and Analytics (DPA) require license.

Note: The networking setup asks if you need to provide the IP range or you want to give IP manually and give subnet mask and validate

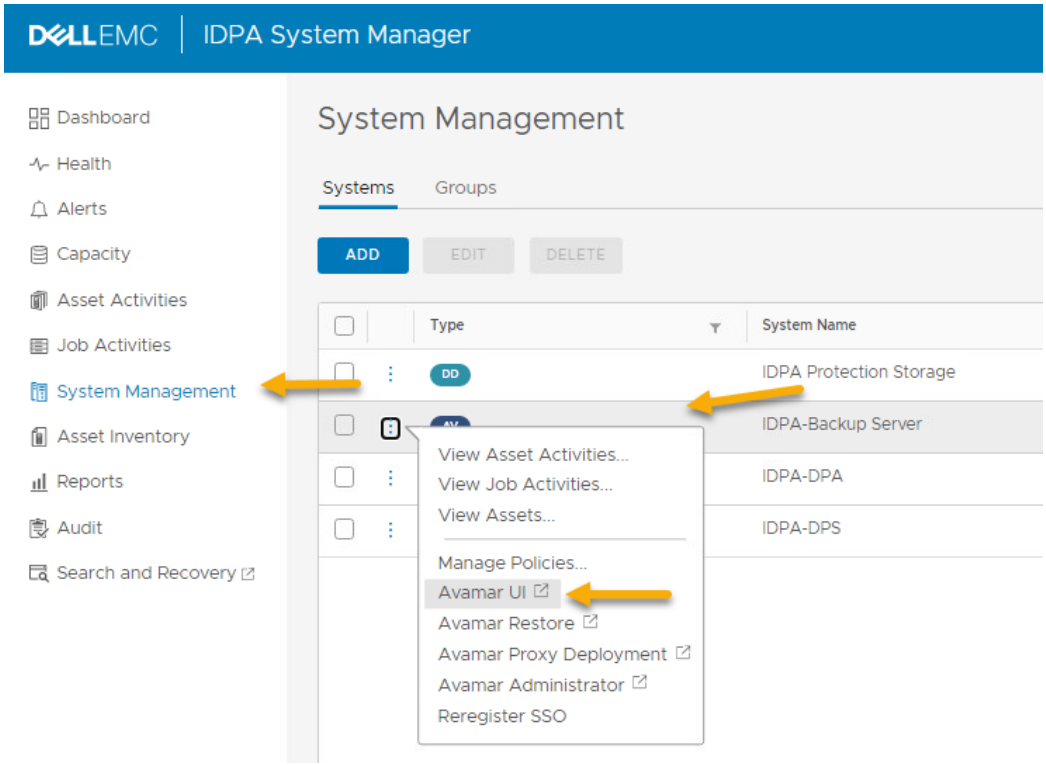
3 Protecting VMware Workloads

IDPA uses Avamar which is proven backup and recovery software that delivers secure data protection for cloud, remote office and data centers. Avamar has tight integration into VMware interfaces that makes it a great solution for protecting any workloads running in a VMware environment.

To set up VMware Image based backups and to protect VMware workloads, VMware vCenter is registered with IDPA. It is one-time process and associated virtual machines are added dynamically to the backup policy. The Proxy is deployed for offloading snapshot workloads and to perform file level recovery from Image level backup. The policy is set and assign dataset a schedule and a retention period.

3.1 Navigating to Avamar UI

1. Login to **IDPA System Manager** using default Idpauser credentials
2. Click on **System Management** on the left pane
3. Under **Systems**, click on three dots to expand IDPA-Backup Server
4. Click on **Avamar UI**

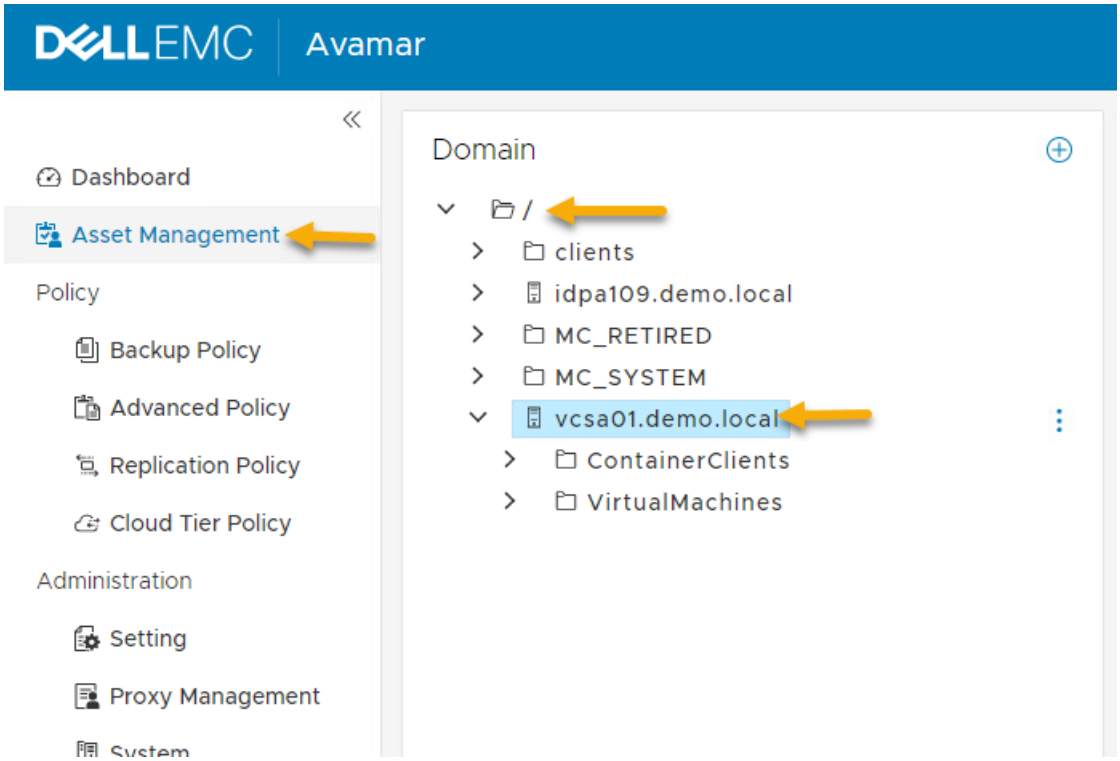


3.2 Register vCenter with IDPA

Following are the steps to add/register vCenter with IDPA for backup and restore VMs.

1. Login to **IDPA System Manager** and navigate to **Avamar UI**
2. At Avamar UI dashboard, navigate to **Asset Management**
3. Select **ADD CLIENT** and click on three dots to expand

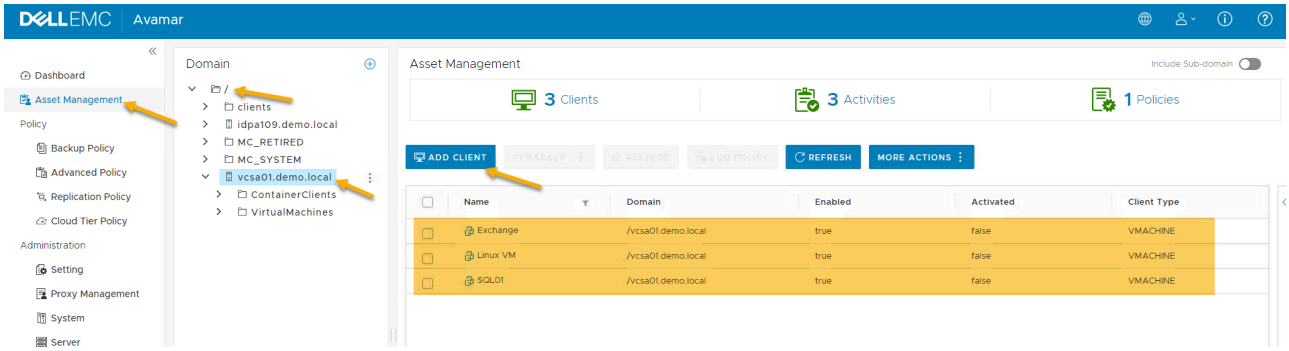
4. Click on Add VMware vCenter
5. Fill the necessary details i.e.
    1) Client Information
        - **Client Type**: Select VMware vCenter from drop down
        - **New Client Name or IP**: FQDN or IP address of vCenter
        - **Client Domain: /**
        - Click NEXT
    2) vCenter Information
        - **Username:** administrator@vsphere.local
        - **Password:** Default password for administrator account
        - **Verify Password:** same password to verify
        - **Port:** 443
        - Click NEXT
    3) Advanced
       This option is to for Auto Discovery, select the suitable option if any, or else click NEXT
    4) Optional Information
       Fill in the details as per the requirement like
        - **Contact**
        - **Phone**
        - **Email**
        - **Location** and click **NEXT**
    5) Summary to verify the inputs and click **ADD**



3.3 Add Virtual Machine as Client to be protected

1. Login to **IDPA System Manager** and navigate to **Avamar UI**
2. At Avamar UI dashboard, navigate to **Asset Management**
3. Click on **Domain** dropdown and select the **vCenter**
4. Select **Virtual Machines**
5. Click on **ADD CLIENT**
    - Select **vCenter** under Host/Cluster section
    - Click on **Datacenter** and select the virtual machines to be protected
    - Click on **SUBMIT**

ss

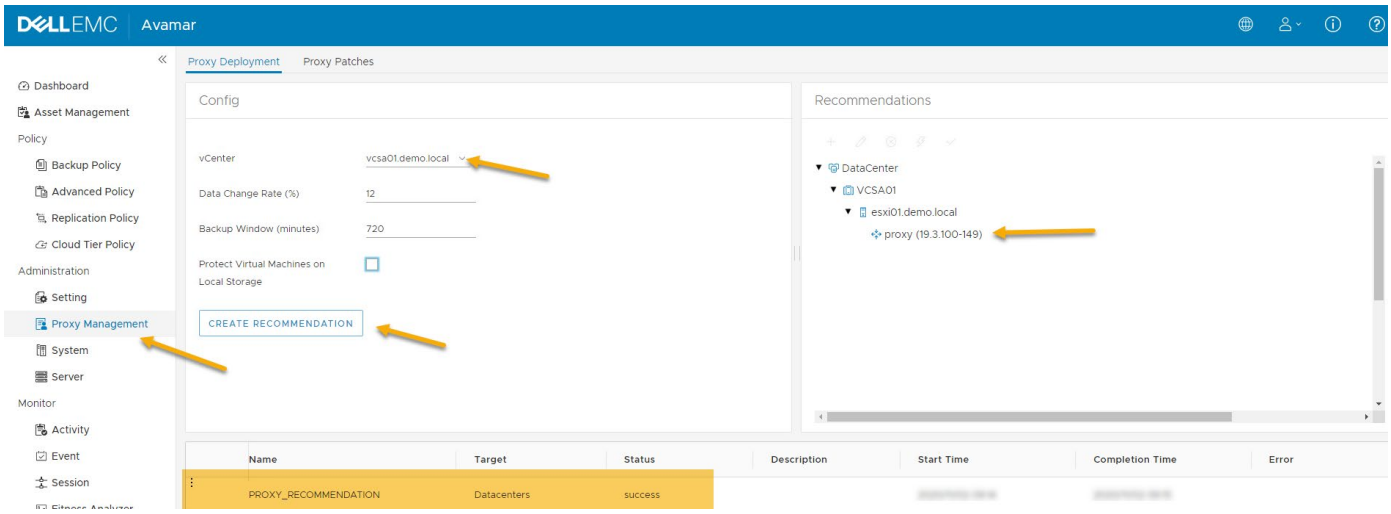


3.4 Proxy Deployment

Avamar Proxy plays the most important role in backup and restore. It is the mechanism behind the backups/restore process. Avamar proxy talks to vCenter API to get the snapshots done of the VM being backed up. Below are the steps to deploy proxy VM on the vCenter.

1. Login to **IDPA System Manager** and navigate to **Avamar UI**
2. At Avamar UI dashboard, navigate to **Administration** on the left pane and click on **Proxy Management**
3. Select **Proxy Deployment**
    1) Under **Config** section, mention the details i.e.
        - **vCenter**: Select vCenter from dropdown
        - **Data Change Rate**:
        - **Backup Window (minutes)**:
        - **Protect Virtual Machines on local storage**: Select this option if VM needs to be on local storage
    2) Under **Recommendations** section, you can create recommendation by clicking on **Create Recommendations,** this creates the internal proxy
        - Click on **DataCenter** dropdown
        - Select vCenter where the proxy gets installed
        - Select ESXi host and click on **+** sign
        - Fill in all the details of proxy VM i.e.
            - **Name:** Name of Proxy VM

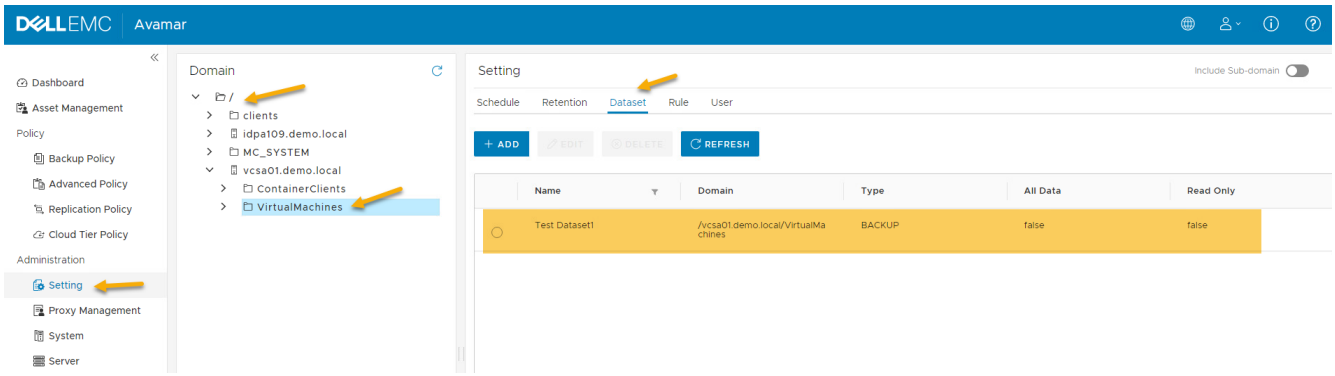
- **Domain: /**<domain>
- **IP:** IP address of the VM
- **Datastore:** Select datastore from the dropdown
- **Network:** Provide the required network (switch)
- **DNS:** <IP address of DNS server>
- **Gateway:** <IP address of gateway>
- **Netmask:** <Mask address>
- **NTP:** <IP address of NTP server>



3.5 Add Dataset

The Dataset is the identification of the content of the backup. Dataset is a filesystem or a directory. Default dataset is inherited from the Avamar group but can be overridden with a specific dataset.

1. Login to **IDPA System Manager** and navigate to **Avamar UI**
2. At Avamar UI dashboard, navigate to **Administration**
3. Click on **Settings**
4. Click on **Domain** dropdown and select the **vCenter**
5. Select **Virtual Machines**
6. Click on **Dataset**
7. Click on **ADD** and provide necessary details
    - **Dataset Name**: <name of the dataset>
    - Select required plugin
    - Options are available to make changes on existing plugin
    - Click on **SUBMIT**

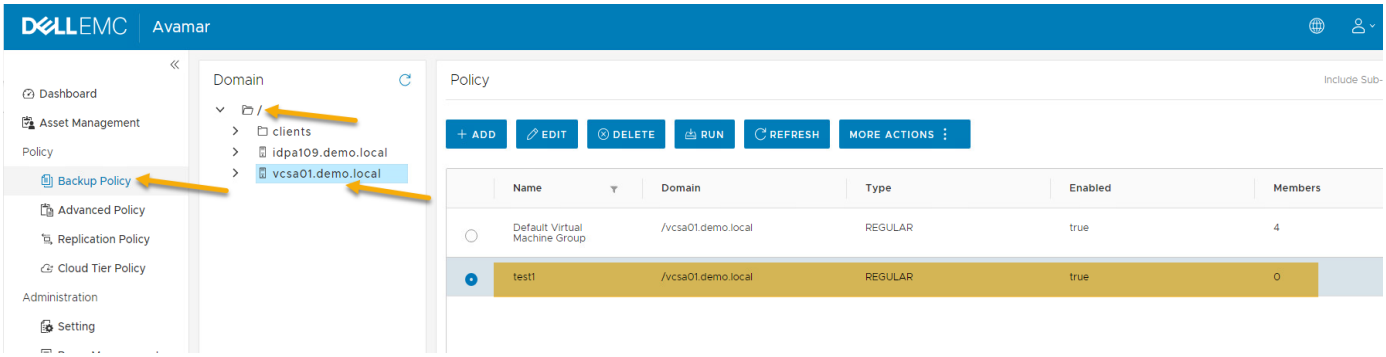


3.6 Backup

The backup policy is created for image level backup and to provide schedule and retention period of a backup.

1. Login to **IDPA System Manager** and navigate to **Avamar UI**
2. At Avamar UI dashboard, navigate to **Policy** and click on **Backup Policy**
3. Click on **Domain** and select **vCenter**
4. Click on **ADD** under Policy section to add new policy
5. Fill in the necessary details
    1. Properties
        - **Name**: Name of the policy
        - **Enabled:** This option is checked when the policy is enabled and to disable the policy, uncheck the box
        - **Override Schedule:** Select appropriate option to skip and run next backup
        - **Domain:** Verify the domain i.e. vCenter name
        - **Auto Proxy Mapping**: Uncheck if you are specifying the created proxy and select the proxy option from proxy column
        - Click **NEXT**
    2. Members
        - Select the domain where virtual machine is added.
        - Select the VM to be protected
        - Enable dynamic rule if you have any
        - Click **NEXT**
    3. Dataset
        - **Dataset**: Select Dataset from dropdown e.g. New
        - **Dataset Name**: Name of the dataset
        - **Plugin Filter:** Select plugin from dropdown
        - Click **NEXT**
    4. Schedule
        - **Schedule**: Select the schedule from the dropdown and proceed accordingly e.g. New
        - **Schedule Name**: Name of the schedule
        - **Recurrence Type**: Select the recurrence type as per the requirement
        - **Backup Window**: Select the backup window as per the recurrence type
        - Click **NEXT**

5. Retention
    - Select the retention from the dropdown and proceed accordingly
    - Click **NEXT**
6. Cloud DR
   This option is applicable when the backup is using cloud platform to save the backup data. Enable this option if you have Cloud DR target available
7. Summary
8. Click **FINISH**



Note: There are options like Edit, Delete, Run, refresh and more for a created policy. In order to test the policy, you can Run the backup anytime. To view the activity and the progress, you can monitor under activity section.

3.7 Restore

Below steps is for the instant access feature of IDPA

1. Login to **IDPA System Manager** and navigate to **Avamar Restore UI**
2. At Avamar Restore UI dashboard, navigate to **Asset Management**
3. Click on **Domain** and Select the **vCenter**
4. Select the domain where the virtual machine is added
5. Select the virtual machine under clients to perform the instant restore
6. Click on **RESTORE** to initiate restore process and select the appropriate from the list
    1. **Backup List**: this is the list of backups performed and saved on the protection storage
    2. **Content:** The content is the list of hard disks (VMDK). You can toggle if you need to perform file level restore. Select the **Hard Disk (VMDK)** to perform restore
    3. **Basic Config:** Select the **Instant Access** option from dropdown under Destination
    4. **Advanced Config:**
        - **vCenter**: Select the target vCenter from the dropdown
        - **VM name:** Provide new name to the VM
    5. **Location**: Select the **datacenter** of the vCenter as location where the virtual machine is restored and then select **ESXi** host
    6. **Resource Pool**: Select required resource pool
    7. **Summary**: Verify if the summary is correct and click FINISH

    Click on View Activity to view the progress Verify the virtual machine is restored at the vCenter by logging in to the vCenter.

A Technical support and resources

Dell.com/support is focused on meeting customer needs with proven services and support.

Storage technical documents and videos provide expertise that helps to ensure customer success on Dell Technologies storage platforms.

A.1 Related resources

Dell EMC IDPA
https://www.delltechnologies.com/en-in/video-collateral/demos/microsites/mediaplayer-video/2018/what-is-dp4400.htm

Dell EMC IDPA Spec Sheet DP4400
https://www.delltechnologies.com/resources/en-us/asset/data-sheets/products/data-protection/h17232-ss-integrated-data-protection-appliance-dp4400.pdf