PURESTORAGE®
Uncomplicate Data Storage, Forever

REFERENCE ARCHITECTURE

FlashBlade with Commvault Cloud: Deployment Guide

Deployment Guide for Pure Storage® FlashBlade® with Cisco UCS C220 M6.

Contents

Introduction

This guide is intended to help IT professionals deploy Cisco Unified Computing System (UCS) C220 M6 servers with Commvault Cloud software and Pure Storage® FlashBlade® storage in a Pure Storage validated reference architecture. The guide covers hardware profiles, operating system and software installation, FlashBlade storage configuration, object lock, and environment expansion.

Please review the related design guide for specifications on the Cisco and Pure Storage hardware.

Prerequisites

Before beginning the procedures in the following sections, make sure you have:

- Two or more Cisco UCS C220 M6 servers, as described in the design guide, racked and physically connected to the network
- Firmware should be updated to current levels
- An existing CommServe server running Commvault release 2023E or higher, version 11.32.15 or later
- A Pure Storage FlashBlade//S200 running Purity//FB 4.1.9 or later; 4.3.4 or later recommended
- FlashBlade racked and physically connected to the network
- One or more subnets and data virtual IP addresses (VIPs) configured
- VIP(s) resolvable using domain name system (DNS)
- Recommended: Apply an array certificate signed by a trusted certification authority (CA), as detailed in Appendix A
- A Rocky Linux 8 Minimal ISO image file, available on rockylinux.org.

NOTE: If the servers will not have Internet access, download the DVD ISO image instead.

- Contact Pure Storage Support to get onboarded for SafeMode™

NOTE: You can refer to Appendix G for resolution to common issues.

Cisco UCS Configuration

Before installing the operating system, you must create a RAID 1 volume from the M.2 SATA SSD drives for the boot disk and enable virtual media to access the installation image.

Boot RAID Configuration

You can create the boot RAID volume either directly using the server's BIOS (system setup) or Cisco Integrated Management Controller (CIMC), or through system profiles in Cisco UCS Manager or Cisco Intersight. Configuration procedures differ between Cisco's management tools, so this guide does not include step-by-step instructions. Table 1 contains links to Cisco documentation for different methods.

Interface	Guide Location
BIOS	Configure Boot with HW RAID on C-Series M6 Servers (refer to the bottom of the page)
CIMC	Configure Boot with HW RAID on C-Series M6 Servers
UCS Manager	Find *Cisco UCS Manager Storage Management Guide* on the Configuration Guides page
Intersight	Refer to "Creating a Storage Policy" under SR-IOV: Supported Combinations and Known Limitations in *Cisco Intersight Managed Mode Configuration Guide*

TABLE 1 Documentation links for boot RAID configuration

Enable Virtual Media

The deployment process requires the use of virtual media. If you use Intersight to manage UCS servers, your server profile may have a virtual media policy that disables virtual media access in the virtual keyboard, video, and mouse (vKVM) interface. To be able to connect the Rocky Linux ISO, you must enable virtual media. Refer to "Creating a Virtual Media Policy" under SR-IOV: Supported Combinations and Known Limitations in *Cisco Intersight Managed Mode Configuration Guide* for more information.

Create UCS Virtual Interfaces

Before installing Linux, you must create virtual networking interfaces to handle data traffic. This includes both virtual network interface cards (vNICs) for Ethernet and virtual host bus adapters (vHBAs) for fibre channel (FC) traffic. See the Configure Networking section to determine how many vNICs you need to create. If you plan to use FC, you should always create two vHBAs, unless you plan to use physical HBAs.

You can use server profiles in UCS Manager or Intersight to configure vNICs and vHBAs. Table 2 contains links to relevant Cisco documentation for each interface.

Interface	Guide Location
UCS Manager	Refer to Network-related Policies in Cisco UCS Manager Network Management Guide, Release 4.3
Intersight	Refer to "Creating a LAN Connectivity Policy" under Supported UCS Server Policies in *Cisco Intersight Managed Mode Configuration Guide*

TABLE 2 Documentation links for virtual interface configuration

Rocky Linux

Obtain the Rocky Linux installation ISO from the Rocky Linux download page and store it in a location accessible from UCS Virtual Media.

Attach ISO

Access the vKVM interface for the C220 M6 server. Use the Virtual Media menu to map the Rocky Linux ISO as a vKVM-mapped vDVD. Boot the server, then wait for the installer to start.

GUI installer

On the Welcome to Rocky Linux 8.8 installer screen, select the language you wish to use, then click the Continue button.

NOTE: This guide uses United States English.

Configure Storage

You will be creating the mount points shown in Table 3. This layout aligns with the CIS Level 1 security policy.

Mount Point	Volume or Partition	Size	Type	File System
/home	rl-home	4GiB	LVM	xfs
/boot/efi	sda1	600MiB	Standard partition	EFI system partition
/boot	sda2	1024MiB	Standard partition	xfs
swap	rl-swap	4GiB	LVM	swap
/var	rl-var	10GiB	LVM	xfs
/var/log	rl-var_log	10GiB	LVM	xfs
/var/log/audit	rl-var_log_audit	4GiB	LVM	xfs
/var/tmp	rl-var_tmp	4GiB	LVM	xfs
/tmp	rl-tmp	4GiB	LVM	xfs
/	rl-root	750GiB	LVM	xfs

TABLE 3 Storage configuration

From the main installer screen, click the Installation Destination link in the System section to open the Installation Destination screen.

From the Installation Destination screen, in the Local Standard Disks section, locate the virtual volume with the device name of “sda” and select it. You may need to scroll to the right to find it. For the Storage Configuration option, select the Custom radio button. Click the Done button at the top of the screen to continue to the Manual Partitioning screen.

From the Manual Partitioning screen, click the link labeled “Click here to create them automatically.” This will populate a set of standard partitions.

The installer will allocate all available space on the disk, so you will need to resize the /home and / mount points before you can create additional mount points. To resize a mount point, select it in the list, then change the Desired Capacity field to the correct value from Table 3. Click the Update Settings button to commit the change.

You can then create the additional mount points. To create a mount point, click the plus (+) button below the list of mount points. In the dialog box that appears, enter the mount point name and desired capacity based on Table 3.

When the list contains all the mount points in Table 3, click the Done button. Review the Summary of Changes dialog box, then click the Accept Changes button to return to the main installer screen.

Configure Networking

You will create one or more bonded network interfaces to provide load balancing and redundancy. If you use virtual local area networks (VLANs) to segregate traffic, you will also create virtual adapters to enable VLAN tagging. Table 4 shows the supported bonding configurations.

Configuration	VLAN tagging	Required vNICs	Logical Adapters	IP Address(es) Bound To
Segregated client and storage networks	No	4	2x Bond	Bond
Segregated client and storage networks with VLAN trunking	Yes	4	2x Bond 2x VLAN	VLAN
Separate client and storage VLANs, single bond	Yes	2	1x Bond 2x VLAN	VLAN
Shared client and storage network	No	2	1x Bond	Bond

TABLE 4 Supported network bonding configurations

You can choose from three supported bonding modes based on what best fits your needs. Table 5 describes the bonding modes.

Display Name	Mode Number	Internal Name	Description
Adaptive load balancing (preferred mode)	6	balance-alb	Balances inbound and outbound traffic between physical ports. Gives the best bandwidth utilization but may not work in all environments.
Adaptive transmit load balancing	5	balance-tlb	Balances outbound traffic between physical ports. Inbound traffic all routes to one port, second port provides failover. Improves some performance..
Active backup	1	active-backup	Most compatible but offers no bandwidth benefits.

TABLE 5 Supported bonding modes

NOTE: See UCS B-Series/C-Series/S-Series/HyperFlex-Series Teaming, Bonding Options with the Cisco VIC Card for more information about Linux bond modes supported on UCS servers.

From the main installation screen, click the Network & Host Name link to access the network settings.

In the hostname field, enter the fully qualified domain name (FQDN) for the MediaAgent. This name must match the DNS entry for the primary IP address.

Disable IPv4 and IPv6 on all vNIC adapters. To edit the adapter, select it in the list, then click the Configure button to open the editing dialog box. On both the IPv4 Settings and IPv6 Settings tabs, choose Disabled from the Method dropdown. Once you have updated both protocols, click the Save button.

Creating Bond Interfaces

Create bond interfaces to provide redundancy. Depending on the topology you want to create, you may end up with one or two bonds. To provide redundancy, ensure that the interfaces you are bonding are connected to separate network switches.

To create a bond interface, click the plus (+) button below the adapters list. From the Add Device dialog box, select Bond in the dropdown, then click the Add button.

In the form that appears (Figure 1), enter the options on the Bond tab as follows:

- In the Interface name field, enter bond0 for the first bond or bond1 if you are creating a second bond.
- Add bonded connections for the appropriate ports.
- From the Mode dropdown, select the bonding mode you want based on Table 5.
- If you select the Active backup mode, optionally enter the name of the adapter that should be primary.
- If you wish to use jumbo frames, enter 9000 in the MTU field. Make sure all network devices between the server and FlashBlade, including the data subnet on the FlashBlade, are configured with a matching MTU.
- If you are not using VLAN trunking and tagging, configure an IPv4 or IPv6 address for the bond.

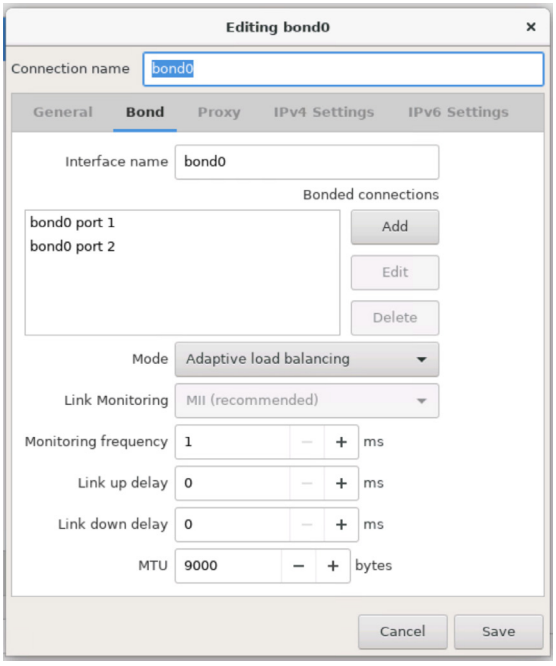

FIGURE 1 Completed bond configuration form

Adding Bonded Connections

When you click the Add button on a new bond, you will be prompted to create a new connection. From the Choose a Connection Type wizard, select Ethernet, then click the Create button. A form similar to the bond creation form will appear.

From the form's Device dropdown, select the device for the port you are bonding. You can use the MAC addresses to identify the ports. Optionally, you can change the settings for cloned MAC address, MTU, Wake on LAN, and link negotiation. When complete, click the Save button to return to the bond creation form.

Repeat for each port you are adding to the bond.

Creating VLAN Interfaces

If you are using VLANs to segregate network client and storage traffic and trunk multiple VLANs to the MA's switch ports, you must create virtual interfaces to tag traffic with the appropriate VLAN ID. Each interface will have its own IP address and use a separate VLAN ID.

You can create VLAN interfaces from the Network & Host Name page by clicking the plus (+) button below the interface list. From the Add device dialog box, select VLAN from the dropdown, then click the Add button.

Complete the VLAN tab:

- Enter a name for the connection in the Connection name field. Pure Storage recommends following the vlan<VLAN ID> convention. For example, an interface for VLAN 100 would be named vlan100.
- Select the bond interface from the Parent interface dropdown.
- Enter the VLAN number in the VLAN id field.
- Enter a name for the interface in the VLAN interface name field. We recommend following the vlan<VLAN ID> convention.

Configure IPv4 or IPv6 addresses on your VLAN interfaces.

Configuring IP Addresses

IP addresses can be assigned to bonds or VLAN interfaces depending on your environment. Refer to Table 2 above to determine which interface(s) should have IP addresses.

If you are using IPv4 addressing, complete the IPv4 Settings tab:

- Select Manual from the Method dropdown.
- Click the Add button to add an address entry, then enter the IP address, netmask, and gateway information.
- If this interface should handle name resolution, enter your DNS server addresses in the DNS servers field.
- If this interface should handle name resolution, enter the appropriate search domains in the Search domains field.
- Enable the checkbox labeled Require IPv4 addressing for this connection to complete.
- If you need to configure custom IP routing, click the Routes button, then enter the appropriate route information.
- On the IPv6 Settings tab, select Disabled from the Method dropdown.
- Click the Save button to finish adding the new interface.

Figure 2 shows an example of the completed IPv4 settings.

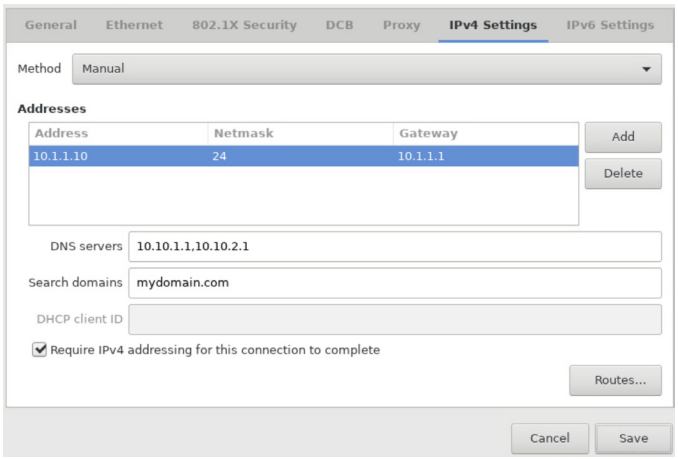

FIGURE 2 Completed IPv4 settings for an adapter

If you are using IPv6 addressing, complete the IPv6 Settings tab:

- Select Manual from the Method dropdown.
- Click the Add button to add an address entry, then enter the IP address, prefix, and gateway information.
- If this interface should handle name resolution, enter the DNS server addresses in the DNS servers field.
- If this interface should handle name resolution, enter the search domains in the Search domains field.
- Enable the checkbox labeled Require IPv6 addressing for this connection to complete.
- If you need to configure custom IP routing, click the Routes button, then enter the appropriate route information.
- On the IPv4 Settings tab, select Disabled from the Method dropdown.
- Click the Save button to finish adding the new interface.

Configure Time and Date

Proper time synchronization between MAs and the CommServe is critical. Clock skew can cause encrypted sessions to fail, disrupting service. Accurate logging also depends on having the correct time set. Configure the time and date settings to avoid these failure scenarios. We strongly recommend configuring the MA to synchronize with network time protocol (NTP) servers.

From the main installation screen, click the Time & Date link to access the time and date settings.

To set the time zone, select your region and city in the appropriate dropdowns at the top of the screen. Optionally, adjust the time and date using the controls at the bottom of the screen.

Optionally, you can configure NTP servers by clicking the gears icon in the top right corner. In the dialog box that appears, enter the DNS name or IP address for any custom NTP servers you wish to add. If you enter a name that resolves to a pool of NTP servers, enable the checkbox under the name field. Click the plus (+) button to add the NTP server. You can remove an existing server by clearing the associated checkbox in the Use column. When you have finished editing the NTP server list, click the OK button to save the changes.

If the Network Time toggle button is set to Off move it to the On position to start NTP synchronization.

Click the Done button to return to the main installation screen.

Add AppStream Repository

The security profile requires packages that are not included in the minimal ISO. You must add the AppStream repository to install those packages.

From the main installation screen, click the Installation Source link to access the repository settings.
Complete the fields as follows:

- Select the ISO file option, then select the Auto-detected installation media option.
- Under the Additional repositories list, click the plus (+) button.
- In the Name field, enter AppStream.
- From the URL dropdown, select https://.
- In the URL field, enter download.rockylinux.org/pub/rocky/8/AppStream/x86_64/os.
- Select the repository URL from the dropdown list.

Click the Done button to return to the main installation screen.

Set the Root Password

Commvault relies on the root account for some of its services. You must enable the account by assigning it a password.

From the main installation screen, click the Root Password link to access the root password setting. Enter a strong password in both fields, then click the Done button.

Create a User Account

We recommend creating a separate, non-root user account for performing administrative functions.

From the main installation screen, click the User Creation link to access the Create User form. Enter a name for the user in the Full name field. The User name field will automatically populate. Enable the Make this user administrator and Require a password to use this account checkboxes. Enter a strong password in both the Password and Confirm password fields. Click the Done button to commit the changes.

Select Minimal Software Install

The default software selection includes more features than Commvault needs, increasing the attack surface of the MA. Changing the software selection to the minimal install will improve security.

From the main installation screen, click the Software Selection link to access the Software Selection form. In the Base Environment list, select the Minimal Install option. Do not enable any of the checkboxes in the Additional software for the Selected Environment list. Click the Done button to commit the change.

Choose Security Policy

To improve the security of the MA, you will choose the Center for Internet Security (CIS) Level 1 server benchmark for Red Hat Enterprise Linux 8.

From the main installation screen, click the Security Policy link to access the Security Policy form. In the profile list, locate and select CIS Red Hat Enterprise Linux 8 Benchmark for Level 1 - Server, then click the Select Profile button.

Once the profile checks have completed, click the Done button to confirm the profile.

Begin the Installation

You are now ready to begin the installation. Click the Begin Installation button to start the process, then wait for the system to boot to the login prompt.

Post-installation Tasks

There are several post-installation configuration steps you must complete. You can quickly make these changes at the command line. Log into the MA using your admin account to complete the setup process.

NOTE: You will be forced to change the admin account password on first login.

Add fail_over_mac Option to Bond Configuration

The bond configuration change you made during installation to add the fail_over_mac option does not carry over to the installed OS. You must add the configuration back after installation. As during installation, you can use the nmcli command to update the configuration.

```
sudo nmcli connection modify <bond name> +bond.options “fail_over_mac=1”
```

For example, to update bond0, you would enter:

```
sudo nmcli connection modify bond0 +bond.options “fail_over_mac=1”
```

Restart networking after updating all bonds.

```
sudo nmcli networking off; sudo nmcli networking on
```

Install OS Updates

You should install all available OS updates before proceeding.

```
sudo dnf update -y
```

Install Required Packages

The solution requires you to install several additional software packages that are not available individually in the installation interface.

The required packages are listed in Table 6.

Package Name	Summary
gcc	Various compilers (C, C++, Objective-C, ...)
nfs-utils	NFS utilities and supporting clients and daemons for the kernel NFS server
policycoreutils-devel	SELinux policy core policy devel utilities
python3	Python 3 interpreter
python3-devel	Libraries and header files needed for Python development
python3-libselinux	SELinux python 3 bindings for libselinux
selinux-policy-devel	SELinux policy devel
tar	A GNU file archiving program

TABLE 6 Required additional software packages

You can install all the required packages with the following command.

```
sudo dnf install -y gcc nfs-utils policycoreutils-devel python3 python3-devel python3-libselinux selinux-pol-
icy-devel tar
```

Create NVMe Drive Arrays

To ensure availability and resilience, you must create RAID-1 arrays for the pairs of NVMe drives. You will use one array for the deduplication databases (DDBs), and the other will house the index cache. You can create the arrays using the following commands.

```
sudo mdadm -C /dev/md/md0 /dev/nvme[0-1]n1 -n 2 -l 1 -e default
sudo mdadm -C /dev/md/md1 /dev/nvme[2-3]n1 -n 2 -l 1 -e default
```

Create Logical Volume Manager Configuration

You will need to create the logical volume manager (LVM) configuration on top of the newly created RAID arrays. The following commands will create a physical volume for each array, as well as separate volume groups and logical volumes for the DDB and index cache. Reserved space in the volume group allows for LVM snapshots when the DDBs and index are backed up.

```
sudo pvcreate /dev/md/md0 /dev/md/md1
sudo vgcreate cvddb /dev/md/md0
sudo lvcreate -n ddb -l 80%FREE cvddb
sudo vgcreate cvidx /dev/md/md1
sudo lvcreate -n idx -l 80%FREE cvidx
```

Create DDB and Index File Systems

The following commands will create XFS file systems on the new logical volumes.

```
sudo mkfs.xfs /dev/cvddb/ddb
sudo mkfs.xfs /dev/cvidx/idx
```

Mount File Systems

Next, you need to mount the file systems and update the /etc/fstab file so they mount during reboots. The following commands will mount the DDB file system to /cvddb and the index cache file system to /cvindex and insert the paths into fstab.

```
sudo mkdir /cvddb
sudo mkdir /cvindex
sudo mount /dev/cvddb/ddb /cvddb
sudo mount /dev/cvidx/idx /cvindex
sudo sh -c 'cat /proc/mounts | egrep "(ddb|idx)" >> /etc/fstab'
```

Configure Python 3

To configure Commvault ransomware mitigation, you must have Python 3 installed and linked at /usr/bin/python. You must also have the psutil Python library installed. The following commands will create the link and install psutil.

```
sudo ln -s /usr/bin/python3 /usr/bin/python
sudo python -m pip install psutil
```

Configure Firewall Ports

By default, the host firewall will block the ports Commvault uses. The following commands will create a firewall service definition for Commvault and allow traffic on its ports.

```
sudo firewall-cmd --new-service=commvault --permanent
sudo firewall-cmd --permanent --service=commvault --set-description="Commvault tunnel"
sudo firewall-cmd --permanent --service=commvault --add-port=8400/tcp
sudo firewall-cmd --permanent --service=commvault --add-port=8403/tcp
sudo firewall-cmd --permanent --zone=public --add-service=commvault
sudo firewall-cmd --reload
```

NOTE: If you use iSCSI and IntelliSnap, you also need to install and enable iSCSI services and connect to the primary array. Please see Appendix D for more information.

FlashBlade Configuration

You will use a Commvault workflow to provision object storage on FlashBlade. This requires an API token for Commvault to use to access the FlashBlade. You will store the token in the credential vault within Commvault. You can create the token for the built-in pureuser account or an external account you've added to the array. The account you choose must have at least the Storage Admin role assigned to it.

We strongly recommend that you apply an array certificate that is signed by a trusted certification authority (CA) to ensure communication is properly encrypted with transport layer security (TLS). See Appendix A for more information. You can configure Commvault to bypass certificate validation; however, this weakens the security profile of the solution and is not recommended.

If you have multiple FlashBlade clusters, such as FlashBlade//S™ and FlashBlade//E™, you need to create an API token on each one.

Create API token

In the FlashBlade GUI, navigate to the Settings tab, then click the Users item in the Security section. From the Users tile, locate the account you want to use. click the more (3-dot) button, then click Create API Token.

In the Create API Token dialog box that appears, you should enter an expiration time for the API token in the Expires In field, but this is not required. Click the Create button to generate the token.

The API Token dialog box will appear, showing a summary of the token details. Click the Copy button to copy the token to the clipboard, then click the Close button to return to the user list.

NOTE: You can view the token later if you need to copy it again.

Add API Token to Commvault Credential Vault

Open Commvault Command Center and log in as an account with permissions to manage credentials. Navigate to the Manage/Security page, then click the Manage credentials tile.

From the Manage credentials page, click the Add link to open the Add credential form. Complete the form as follows:

- From the Account type dropdown, select Storage Array Account.
- Accept the default BUILT_IN in the Credential Vault dropdown, unless you have a supported third-party vault connected to Commvault that you wish to use.
- In the Credential name field, enter a meaningful display name for the credential.
- In the user account field, enter the username associated to the API token. If you are using an Active Directory account, make sure to include the domain name.
- In the Password field, paste the API token you copied from the FlashBlade.
- Optionally, in the Description field, enter a description to help you identify the token.
- Click the Save button to create the credential.

Repeat the procedure for each FlashBlade.

Deploy Commvault MediaAgent

To deploy the MediaAgent, you must install the MediaAgent software, enable ransomware protection, tune the configuration, and create storage pools.

Install MediaAgent software

Commvault supports multiple software deployment options; however, this document will describe remotely installing the MediaAgent using Commvault Command Center.

In Commvault Command Center, navigate to the Manage/Servers page. Click the Add server link to open the Install software form. Complete the form as follows:

- Select the option to install software packages.
- In the Host name field, enter the DNS name or IP address of the MediaAgent you are installing. You may enter additional hosts to deploy multiple MediaAgents, provided the user login credentials are the same.
- From the OS Type options, select Unix and Linux.
- If you have a saved credential you wish to use, enable the Use saved credentials slider, then select the correct credential. Otherwise, leave the slider disabled.
- If you do not use a saved credential, enter your admin account in the username field. Do not use the root account, as it will be unable to connect to the MA.
- If you do not use a saved credential, enter the password for the admin user in the Password and Confirm password fields.
- From the Select package(s) dropdown, select the Media Agent item.

Click the Install button to begin the installation. You can monitor progress from the Jobs page.

Enable Commvault Ransomware Protection

Once the installation has completed, you need to enable Commvault ransomware detection. Connect to the Linux terminal as the admin user. Run the following commands to enable Commvault ransomware protection.

```
sudo su
cp /etc/fstab /etc/fstab.backupfile
cd /opt/commvault/MediaAgent64
./cvsecurity.py enable_protection -i Instance001
reboot
```

The MediaAgent will reboot. When it is back online, log in again, and elevate to root. Run the following commands to finish updating Commvault.

```
sudo su
cd /opt/commvault/MediaAgent64
./cvsecurity.py restart_cv_services -i Instance001
```

You can confirm that SELinux is in enforcing mode by running the sestatus command:

```
[root@sn1-x210c-h08-commvault01 MediaAgent64]# sestatus
SELinux status:                 enabled
SELinuxfs mount:                /sys/fs/selinux
SELinux root directory:         /etc/selinux
Loaded policy name:             targeted
Current mode:                   enforcing
Mode from config file:          enforcing
Policy MLS status:              enabled
Policy deny_unknown status:     allowed
Memory protection checking:     actual (secure)
Max kernel policy version:      33
```

Repeat the entire process for all MediaAgents you are deploying.

MediaAgent Tuning

For the best performance, you need to change some of the default MediaAgent settings. You can access the configuration options from Commvault Command Center.

Navigate to Manage/Infrastructure, then click the MediaAgents tile. From the MediaAgents list, click the name of the MediaAgent you want to modify.

Parallel Data Transfer Operations

Locate the Control tile, then click the edit icon next to Parallel data transfer operations. Change the value to 200, then click the Submit button.

Maximum Concurrent Upload Threads

In the Settings tile, click the edit icon next to Configure number of concurrent upload threads for cloud storage. Set the value based on the number of chassis in your FlashBlade//S, using 50 connections per chassis. For example, for a FlashBlade//S with three chassis, you would set the concurrent threads to 150.

NOTE: Performance varies based on a number of environmental factors. You may see better backup speeds with a higher or lower setting.

Index Cache location

You need to move the index cache from its default location to the NVMe drive arrays you created during Linux post-install configuration. In the Index Cache tile, click the edit icon. In the Edit Index Cache Properties dialog box that appears, change the Index cache path field to /cvindex, then click the Save button.

Look Ahead Size

For best restore performance, you need to adjust the look-ahead size for the MediaAgent. You must use the SILookAheadAsyncIOBlockSizeKB setting to increase the look-ahead to 768KB. To set the new value, navigate to the Manage/System page. Click the Settings tile. Click the Add dropdown, then select Entity Settings.

From the Add entity settings form, enter SILookAheadAsyncIOBlockSizeKB in the Name field. When the auto search populates, select Set block size used by async IO in Look Ahead reader (SILookAheadAsyncIOBlockSizeKB). The rest of the form will populate automatically.

Complete the Add entity settings form as follows:

- From the Entity dropdown, select the MediaAgent(s) you want to configure. You can apply the setting to as many MediaAgents as you want.
- In the Value field, enter 768.
- In the Comment field, enter a reason for adding the setting.

Click the Save button to commit the change.

Create Storage Pools

You must create storage pools in Commvault to allow it to send data to FlashBlade object storage. A storage pool combines one or more object buckets on FlashBlade with one or more MediaAgents and a deduplication store.

You can use the workflow feature in Commvault to provision object storage on FlashBlade.

NOTE: If you did not apply a signed array certificate, you must disable certificate validation in Commvault to use the workflow. This is not recommended for production implementations; you should apply a certificate signed by a trusted CA.

For information about expanding existing storage pools, please refer to Appendix E.

Install Provisioning Workflow

You can use Commvault Command Center to download and install the workflow from the Commvault store.

Navigate to the Workflows page, then click the Commvault store link. A new browser tab will appear. If you are presented with a login screen, use the same Commvault credentials with which you are logged into the Command Center. Once the store opens, locate the Provision Pure FlashBlade Object Storage workflow. You can filter the list using the search box to help find it more easily. Click the Install button under the workflow icon, then wait for the installation to complete. Return to your Command Center window, then refresh the page to update the list of workflows.

You are now ready to execute the workflow and provision storage on FlashBlade.

Execute Workflow

1. In the Command Center workflows list, locate the Provision Pure FlashBlade Object Storage workflow and click its title. The workflow will present a series of forms that you will complete.
2. Complete the initial workflow form as follows:
   - In the dropdown, select the saved credential containing the API token.
   - In the field, enter the management name or IP address of the FlashBlade//S. If you have applied a signed certificate to the array, make sure the name you enter matches the certificate common name, not the subject alternative name.
3. In the object account form, select the account to store the object users and buckets. If you want to create a new account, select New account and enter the name in the New account name field.
4. On the Select IPs or subnets form, select the option you want to use to restrict privileged bucket access on the FlashBlade//S. You can choose to restrict to MediaAgents, IP subnets, or no restrictions. Selecting MediaAgents will use specific MAs' IP addresses in the access policy. Selecting the IP subnet option will allow access for any IP address on the IP subnets you define. Selecting None will skip the access restrictions and allow any address to use the privileged keys–and is therefore not recommended. **NOTE:** Use the MediaAgents option to provide the highest security level. However, if you deploy the solution with separate client and storage networks, you should choose the IP subnet option to avoid issues stemming from name resolution.
   - If you select MediaAgents, the Select MediaAgents form will appear. Check the boxes for the MediaAgents that need access. Their IP addresses will be added to the policy.
   - If you select the IP subnet option, the IP subnets form will appear. Click the plus (+) button to add a field for each subnet you want to allow. Enter the subnets in x.x.x.x/n format, where x.x.x.x is the IP range and n is the subnet mask bit length.
5. On the bucket details form, enter a name for the bucket you want to create. To enable object lock on the bucket, move the Enable object lock slider to the right. The form has SafeMode retention lock selected by default, but it will not apply unless you also enable object lock. You can disable SafeMode retention lock by moving its slider to the left.

   If you choose to enable object lock, versioning will be disabled on the bucket, and the freeze objects setting will be enabled.
6. The result form will display success or failure. If you wish to create another bucket before exiting, move the slider to the right, click Next, then repeat step 5. To stop creating buckets, move the slider to the left and click Next. **NOTE:** We recommend creating one bucket with object lock disabled and one or more with object lock enabled. If you plan to have multiple object lock retention periods, create a separate bucket for each one.
7. A summary form will show the objects that were created on the FlashBlade//S and in Commvault.

Repeat the workflow for any other FlashBlade arrays where you want to configure object storage for Commvault.

You are now ready to create storage pools in Commvault.

Add Storage Pools

You need to create storage pools for Commvault to manage its data on the FlashBlade. For object lock, you must create a separate pool for each retention period you plan to use. For copies of data that do not use object lock, we recommend creating a single pool and using separate server backup plans to define retention policies.

To create a pool:

In Commvault Command Center, navigate to Storage/Cloud. Click the Add link to open the Add cloud storage form. Complete the form as follows:

- From the Type dropdown, select Pure Storage FlashBlade.
- In the Name field, enter a name for the new pool.
- From the MediaAgent dropdown, select the MediaAgent that will own the pool.
- In the Service host field, enter the DNS name for the FlashBlade data IP address. This name must exist in the subject alternative name field of the FlashBlade array certificate; otherwise, TLS will not fail. You can bypass TLS by entering "http://" at the beginning of the service host name. Alternatively, you can disable certificate validation, but this affects all certificates and is not recommended for production deployments.
- From the Credentials dropdown, select the privileged credential the workflow created.
- In the Bucket dropdown, enter the name of the FlashBlade object bucket. You should create storage pools that will not use object lock first.
- In the Deduplication DB location section, enable the Use deduplication slider, then click the Add link
- Complete the Add Deduplication DB location popup dialog box as follows:
- From the MediaAgent dropdown, select the MediaAgent that will host the partition.
- In the Deduplication DB location field, enter or browse to the path for the database. For best performance, enter a path under /cvddb so the database is placed on NVMe storage.
- Click the Add button to add the new database partition to the form.

NOTE: You can add up to four partitions. For best performance, you should have at least one partition on each MediaAgent in the storage pool.

Click the Save button to submit the form and create the pool.

Repeat this process to create a storage pool for each bucket you created. For each pool's deduplication DB location, enter a different path under /cvddb.

If you are adding a pool that will use FlashBlade//E, refer to Appendix B for additional considerations. For information about adding Commvault Air Gap Protect, refer to Appendix F.

Decrease Deduplication Block Size

For the best balance of storage efficiency and performance, you need to reduce the deduplication block size to 128 KB for each of the storage pools you created. As of Commvault release 2023E, you can only manage block size using Commvault CommCell Console.

NOTE: Commvault release 2024 requires an approval code from Commvault to enable the CommCell Console.

To modify the block size:

1. In the CommCell Console, locate the Storage Resources node in the CommCell Browser tree and expand it. Click the Storage Pools node.

NOTE: If the console was already open, you may need to refresh the view to see the pools you created.

2. Right-click the pool, then click Properties>Storage Pool. The Storage Pool Properties dialog box appears.
3. On the Advanced tab, change the Block level Deduplication factor to 128 KB, then click the OK button.
4. Enter the confirmation text in the dialog box that appears, then click the OK button.

Repeat steps 2 and 4 to change the block size on all FlashBlade storage pools.

Share Buckets

To allow multiple MediaAgents to process backups to FlashBlade in parallel, you must share the bucket with those MediaAgents. You can share the bucket using Commvault Command Center.

To share the bucket:

1. In Command Center, navigate to Storage/Cloud. In the list of storage pools, click the name of the pool you wish to change to access the pool settings.
2. In the Bucket table, click the Actions button (three dots) for the bucket to share. Select Add MediaAgent from the menu that appears. The Add MediaAgent form appears.
3. On the Add MediaAgent form, enable the checkboxes next to the MediaAgents that should have bucket access, then click the Save button.

NOTE: Make sure you all the MediaAgents are allowed in the FlashBlade object access policy; otherwise, sharing the bucket will fail.

Repeat the procedure to share any other FlashBlade buckets in the storage pool, and for any other FlashBlade storage pools.

Set Storage Accelerator Credentials on Buckets

Setting a credential for Storage Accelerator lets you restrict where your privileged access keys are used and improves your security posture. Even if you do not intend to use Storage Accelerator, we recommend setting a credential for it. You can set Storage Accelerator credentials using Commvault Command Center. You have to set the credential on each bucket in a pool.

To set the credential:

1. In Command Center, navigate to Storage/Cloud. In the list of storage pools, click the name of the pool you wish to change to access the pool settings.
2. On the pool page, click the name of the bucket in the Buckets tile to open the bucket properties.
3. From the Configuration tile, click the Storage accelerator credentials dropdown, then select the unprivileged credential the workflow created. Click the checkbox to apply the change.

Repeat the procedure for all buckets in all FlashBlade storage pools.

Optional: Enable Object Lock Support on Storage Pools

For Commvault to manage object locking, you must enable the Hardware WORM setting on the storage pool and set a retention period for it. This will then apply to any destination copy in a server backup plan or storage policy.

Please see Appendix C for detailed configuration instructions.

Configure Server Backup Plan

Before you can protect data to FlashBlade, you need the storage pool associated with a server backup plan or storage policy. Depending on your needs and how you intend to use FlashBlade, you can create a new plan or policy, or you can add it as a new target in an existing plan or policy. This guide will only cover server backup plans.

To create a new plan:

1. In Commvault Command Center, navigate to Manage/Plans.
2. Click the Create plan link, then select Server backup from the menu to start the Create Server Backup Plan wizard.
3. On the General page, select Create a new plan. Enter a name for the plan in the Plan name field. Click the Next button to continue.
4. On the Backup Destinations page, click the Add Copy button and complete the Add copy form as follows.
   - Optionally, change the copy display name in the Name field.
   - From the Storage dropdown, select the FlashBlade storage pool you created.
   - Adjust the retention period to meet your needs.
   - If this storage pool does not use object lock, you can set extended retention rules.
   - Click the Save button to return to the wizard.
5. The Backup Destinations page will now show the FlashBlade destination you configured. You can add more copies to enable replication to other storage types, other sites, and public cloud storage such as Commvault Air Gap Protect. You can also add copies later. To add a copy now, click the Add copy link, then complete the Add copy form again. Repeat the procedure as many times as you need.
6. When you have added all your desired destinations, click the Next button to continue.
7. On the RPO page, make any changes you want to the scheduling options, then click the Next button to continue.
8. On the Options page, make any desired changes to the snapshot management options.
9. Click the Submit button to create the server backup plan.

Conclusion

By following this guide, you have deployed one or more MediaAgents on Cisco UCS 220 M6 servers, created object storage buckets, and configured Commvault policies to manage your data. You can now run backup and recovery operations, benefiting from the performance and scalability of FlashBlade arrays, Commvault software, and Cisco UCS servers, confident that you are getting the best performance out of your environment.

Additional Resources

- Reference Architecture Design Guide
- Cisco UCS C220 M6 Rack Server support page
- Pure Storage support
- Commvault documentation
- Rocky Linux

Appendix A: Apply Array Certificate

To use TLS securely with FlashBlade object storage, you must apply a certificate to the FlashBlade that is signed by a CA Commvault software trusts. The certificate must include the subject alternative name (SAN) field, and the service host name you configure in the Commvault storage pool must exactly match an entry in the SAN field and be resolvable by the MA. Each FlashBlade requires its own certificate.

You must generate a new certificate signing request (CSR) and private key and have it signed by the trusted CA. You must export the signed certificate and private key separately, in privacy enhanced mail (PEM) format, Base64 encoded. You may encrypt the private key with a passphrase. Refer to the documentation for your chosen tool for instructions on how to create the CSR, private key, and exported files.

To apply the certificate to the FlashBlade:

1. From the Settings page navigation sidebar, click Certificates under Security.
2. Click the More Options button in the Array Certificates panel. The Import Array Certificate pop-up window appears.
3. Complete or modify the following fields:
   - Certificate: Click Choose File and select the signed certificate.
   - Private Key: Click Choose File and select the private key.
   - Intermediate Certificate (optional): Click Choose File and select the intermediate certificate.
   - Key Passphrase (optional): If the private key is encrypted with a passphrase, enter the passphrase.
4. Click Import.

Once the certificate has been imported, Commvault's validation checks will succeed, and you will be able to use TLS to encrypt communication with the FlashBlade.

Appendix B: FlashBlade//E Considerations

The performance and scaling characteristics of FlashBlade//E are different from FlashBlade//S. The process of configuring both in Commvault is the same; however, you should consider the following items:

- **Limiting auxiliary copy streams**: If Commvault will frequently be reading data from FlashBlade//E, for restore, auxiliary copy to cloud, or other uses, consider limiting auxiliary copy streams to 20. This reduces the impact of the auxiliary copies on the read workloads.
- **Concurrent read and write workloads**: Certain parallel read and write workloads can conflict on FlashBlade//E. Write operations tend to take precedence over read operations, limiting their available bandwidth. Commvault tends to prioritize restore streams over backups and other jobs, but auxiliary copy and some other write operations can still affect read performance. You should try to schedule operations to avoid these conflicts.
- **Maximum concurrent upload threads**: FlashBlade//E handles fewer concurrent connections than FlashBlade//S, and that limit scales differently. High parallelism increases latency reported by the FlashBlade//E. It generally will not affect throughput, but it could lead to perceived performance problems. If a MediaAgent is connecting only to FlashBlade//E and not FlashBlade//S, consider setting a maximum of 40 upload threads per control chassis on that MA.

Appendix C: Object Lock

You can enable object lock functionality on a storage pool using Commvault's WORM storage lock feature. Once enabled on a pool, it cannot be disabled. You must create a separate bucket and storage pool for each retention period.

Enabling WORM storage lock requires a single change to the storage pool. To use the pool once it is enabled, you will need to add it as a backup destination in your server backup plans or storage policies, or else create new server backup plans or storage policies.

Prerequisites

Before enabling WORM storage lock, you must enable object lock on the associated FlashBlade bucket(s). If you used the workflow to provision storage as described in the Execute Workflow section, the bucket will already be configured according to best practices.

NOTE: You cannot enable object lock on a FlashBlade bucket after you add it to a Commvault storage pool. Only empty buckets can have object lock enabled, and Commvault will write several objects during pool configuration.

Storage Pool

To enable WORM storage lock on a storage pool:

1. In Commvault Command Center, navigate to the Storage/Cloud page. Locate the FlashBlade storage pool and click its name to open its configuration page.
2. Locate the WORM tile. Move the WORM storage lock slider to the right. The Retention rules dialog box will appear.
3. In the Retention rules dialog box, set the retention period to match your immutability requirement. If any existing server backup plans already use the storage pool, the table will show the changes that will be made to their retention settings. Click the OK button to continue. A confirmation dialog box will appear.
4. In the confirmation dialog box, you must enable both checkboxes and enter the confirmation text. Click the Submit button to complete the change.

After you have enabled WORM storage lock, the WORM tile will show WORM storage lock and Compliance lock as enabled, and both controls will be grayed out. The tile will also show the retention period you defined. You can increase but not decrease retention for the pool, and any changes will apply to all plans and policies that share the storage pool.

Server Backup Plan

Since object locking is enabled at the storage pool and inherits into plans and policies, you can follow the procedure in the Configure Server Backup Plan section to add a locked pool as a backup destination. When you add a WORM-enabled storage pool as a destination in a server backup plan or storage policy, you will not be able to adjust retention because the storage pool controls it.

Appendix D: Installing iSCSI

The Rocky Linux installation procedure in this guide does not install iSCSI services, but you can install and configure iSCSI if you need it to connect to a Pure Storage FlashArray™ or other array. This section will describe how to install and connect an iSCSI initiator from your MediaAgent, but it is not an exhaustive manual. Please refer to the documentation for Rocky Linux and your storage array for more details.

1. Log into the MediaAgent using your admin account.
2. Install the iscsi-initiator-utils package to add the iSCSI client.

```
sudo dnf install -y iscsi-initiator-utils
```

3. By default, the system will assign an iSCSI qualified name (IQN) based on a pseudo-random number. If you prefer a more easily identifiable name, you can change the IQN by editing the /etc/iscsi/initiatorname.iscsi file and changing InitiatorName to a new value. Restart the iscsid service afterward.

NOTE: IQNs must be unique in your environment to avoid accidental data loss and other issues.

```
sudo systemctl restart iscsid
```

4. You should provision storage on your array before attempting to connect to it. FlashArray and some other storage systems block iSCSI clients from connecting if there is no storage assigned to that client's IQN.
5. Discover the array target.

```
sudo iscsiadm -m discovery -t st -p <array discovery portal>
Example: sudo iscsiadm -m discovery -t st -p 10.10.10.100
```

Your MediaAgent should now be connected to the array and able to see the volume(s) presented by the array. You should not need to create or mount any file systems or perform any other provisioning actions.

Repeat steps 4 and 5 for any other arrays you need to connect.

Appendix E: Expanding Storage Pools

As your environment grows, you will need to add capacity to your FlashBlade and add MediaAgents to manage the additional data. You will also need to expand storage pools to use the additional MediaAgents. This appendix describes the necessary steps to grow a storage pool.

FlashBlade Object Access Policy

You must ensure that new MediaAgents can access your FlashBlade object buckets. The FlashBlade object access policy controls this. If you originally chose to limit access to specific MediaAgents, you will need to add your new MediaAgents to the policy. You can either use the provisioning workflow or edit the policy directly on the FlashBlade.

Workflow

To update the object access policy using the Commvault workflow, follow the procedure covered in the Execute Workflow section. When you reach the Select MediaAgents form, you must select all the MediaAgents that will access the bucket, including the ones you granted access to previously.

The changes apply immediately, so you do not need to complete the workflow. When you reach the Enter Bucket Details form, click the Cancel button.

Direct Edit

To edit the object access policy directly, open the FlashBlade management GUI. Navigate to the Policies page, then click the Object Store tab. Locate the mediaagent policy for your object account and click its name. In the Rules tile, locate the maaccess entry. Click its menu button (three dots), then click Edit from the popup menu to open the Edit Rule dialog box.

Locate the Source IPs item, and click the plus (+) button next to it. In the text box that appears, enter the IP addresses of the new MediaAgents, separated by commas. Click the OK button to finish adding addresses.

The Source IPs list will now reflect the new MediaAgents. Click the Save button to close the dialog box and update the object access policy.

Storage Pool

To add the new MediaAgents to the storage pools, you must add the MediaAgents to the bucket configuration in Commvault. You may also want to add or move DDB partitions onto the new MediaAgents to improve deduplication performance.

Add MediaAgents to Bucket

To add new MediaAgents to a bucket, follow the procedure in the Share Buckets section.

Add DDB Partitions

The DDB for a storage pool can have up to four partitions. For best performance, distribute partitions across as many MediaAgents as possible in the storage pool. You should add a partition on each MediaAgent you add to an existing pool, unless the pool already has four MediaAgents with DDB partitions. You must use the CommCell Console to move DDB partitions.

NOTE: Make sure to suspend or kill any backup or auxiliary copy jobs using the storage pool before you make changes.

To add a DDB partition:

1. In the CommCell Browser pane, expand Storage Resources, then Deduplication Engines.
2. Locate the engine associated with the storage pool you are expanding. Right-click the engine, then select Advanced>Add Partitions from the popup menu.
3. In the Partition Path dialog box, select the new MediaAgent from the MediaAgent dropdown. In the Partition Path field, enter the same path where the DDB was located on the original MediaAgent. Click OK to complete the change.

If you are adding multiple MediaAgents to the storage pool, you can repeat steps 2 and 3 to add more partitions.

Move DDB Partitions

If you add a MediaAgent to an existing storage pool that already has four DDB partitions, and any MediaAgent in the pool hosts more than one partition, you should move a partition to the newly added MediaAgent. You must use the Commvault Console to move DDB partitions.

NOTE: Make sure that no backup or auxiliary copy jobs are running for the storage pool before making changes.

To move a DDB partition:

1. In the CommCell Browser pane, expand Storage Resources, then Deduplication Engines.
2. Locate and expand the engine associated with the storage pool you are expanding.
3. For each DDB node directly underneath the engine, right-click the DDB, then click All Tasks>Move Partitions from the popup menu.
4. In the Move Partition dialog box, locate the partition you want to move and make note of the partition path. Click the Choose Path... link for that partition. You should move the highest numbered partition from the MediaAgent that has the most partitions.
5. In the Partition Path dialog box , select the new MediaAgent from the MediaAgent dropdown. In the Partition Path field, enter the same path where the DDB was located on the original MediaAgent. Click OK to complete the change. If you are adding multiple MediaAgents, you can perform steps 4 and 5 again to move a partition to each new MediaAgent in a single step.
6. From the Move Partition dialog box, click the OK button to begin the move process.
7. In the confirmation dialog box, click the Yes button to begin the move process.

Commvault will execute a Move Partition job, which you can monitor from Job Controller. When the job completes, you can refresh the Deduplication Engines list to confirm that the partition path has been updated.

Repeat this procedure for all DDBs under the same deduplication engine, then repeat the entire process for each storage pool you want to expand.

Appendix F: Commvault Air Gap Protect

To add Air Gap Protect to your environment, you must first contact your Commvault team to obtain appropriate licensing for your environment and apply it to your CommCell.

Follow the instructions in Configuring Air Gap Protect in Commvault documentation to add a storage pool using Air Gap Protect.

After you create the storage pool, you can share the container with other MediaAgents, as you shared the FlashBlade bucket. Click the name of the storage pool to open its configuration page. In the Container tile, click the Action (ellipsis) button for the container, then click Add MediaAgent in the popup menu. In the list of MediaAgents, enable the checkboxes next to the MAs you want to handle data transfers for the storage pool. Click the Save button to complete the change.

You must add the Air Gap Protect pool as a backup destination in a server backup plan or storage policy before Commvault will write any data there. Once added, Commvault will periodically copy new unique data to the pool, on a customizable schedule.

To add a backup destination using Command Center, navigate to the Manage/Plans page. Click the name of the plan you want to modify, then click the Backup destinations tab on the page that opens. Click the Add button above the Backup destinations table, then select Copy from the popup menu. The Add copy form will appear.

Complete the form as follows:

1. In the Name field, enter a meaningful display name for the copy. This does not need to match the name of the storage pool.
2. From the Storage dropdown, select the storage pool you created.
3. From the Backups to copy dropdown, select the appropriate option. You can choose to copy all jobs or only full backups based on a specific frequency.
4. Optionally, from the Source dropdown, you can select a specific storage pool to read new data from. By default, Commvault will use whatever storage pool is just above in the backup destinations. We recommend that you select a FlashBlade//S storage pool as the source.
5. Optionally, you can choose to apply a start date to the copy. Commvault will ignore backups taken before this date. To choose a date, select the Specify a date from when to retain copies option, then enter a date in the Start time field or click the calendar icon to select a date using a calendar tool.
6. If you chose to only copy full backups, choose whether Commvault should copy the first or last full backup for your selected frequency.
7. Use the Retention period controls to set the base data retention for copied backups.
8. If you wish to set different retention periods for some backups, such as keeping monthly full backups for longer, toggle the Extended Retention rules slider, then define the additional rules. You can use the Add link to create more rules.
9. Click the Save button to update the plan.

The plan changes will take effect immediately, and the next time the auxiliary copy schedule runs, it will copy data to Air Gap Protect based on the rules you defined.

Appendix G: Common issues

This appendix covers some common issues you may encounter during deployment and resolutions. If you have an issue that is not covered, or if the listed steps do not resolve the issue, contact customer support for the affected component.

Installation Issues

Table 7 covers common issues during installation.

Symptoms	Resolution
During Rocky Linux installation, the network bond does not start, and the IP address is not reachable from another system.	Try a different bond mode. If it works, check the network switch configurations to confirm they are compatible with the bond mode you tried to use.
Commvault MediaAgent software installation fails to complete.	From the MA terminal, run the following command. `sudo commvault status` In the output, look for the CommServe/Gateway Host Name and CommServe Client Name entries. If they are empty or do not show the actual CommServe name, the MA is unable to resolve the name. Confirm that the MA DNS servers and search domains are correct and that DNS contains both host and reverse lookup records for the CommServe.

TABLE 7 Installation issues

DDB changes

Table 8 covers common issues during DDB changes.

Symptoms	Resolution
When changing the deduplication block size on a DDB, or when adding or moving partitions, you receive an error message stating that garbage collection and journaling are enabled.	This is due to caching behavior in the CommCell Console interface. Exit the console and reload it.

TABLE 8 DDB change issues

PS2587-01-en 04/24