

Commvault in the AWS Marketplace

Version 11 Feature Release 25 (11.25)

September 15, 2021

Contents

Commvault in the AWS Marketplace	4
Intelligent Data Services from Commvault.....	4
What is AWS Marketplace.....	4
Delivery methods.....	4
Pricing Model.....	5
Operating Systems	5
Commvault Solutions in the AWS Marketplace	6
Commvault Software in the AWS Marketplace.....	6
Commvault services in AWS Marketplace.....	6
Getting Started in AWS Marketplace	7
How to create an AWS account	7
How to access AWS Marketplace	7
Locating Commvault Software in AWS Marketplace.....	7
Accepting a Private Offer in AWS Marketplace.....	7
Next Steps.....	8
Requirements	8
General requirements.....	8
System Requirements.....	8
Service endpoints.....	12
AMI usage requirements.....	14
Deploying Commvault in AWS Marketplace	14
Activating your Commvault Support via Amazon Product Connection (PSC)	21
Where to go next.....	22
Other Operations	22
Configuring AWS backups.....	22
Performing AWS restores.....	25
Disaster Recovery for Amazon EC2	27
Monitoring Commvault with AWS CloudWatch.....	28
Using the License Summary Report to understand usage.....	29
Optimizing Commvault in AWS Marketplace.....	34
Terminating Commvault instances in AWS Marketplace.....	35
Commvault and AWS CloudFormation	36

Components Deployed by AWS CloudFormation	36
Use Encryption in AWS Marketplace Products	39
Tagging in AWS Marketplace Products.....	39
Termination Protection.....	40
AMI Drive Layout.....	40
BYOL Deployment.....	42
Commvault Backup & Recovery: Standard Deployment.....	44
Commvault Backup & Recovery: Custom Deployment.....	46
Commvault Backup & Recovery: Additional Deployment	47
Related information	49

Commvault in the AWS Marketplace

Commvault's industry-leading intelligent data management platform provides seamless backup, recovery, disaster recovery, and data insight for cloud-based workloads. Protected workloads include Amazon EC2, EBS, EKS, Aurora, RDS, Redshift, Red Hat OpenShift, S3, DynamoDB, DocumentDB, VMware Cloud on AWS, and Amazon Outposts. Commvault's cloud-native agentless approach orchestrates snapshot creation including cross-region and cross-account replication.

Commvault secures your data management environment using intelligent data protection, and monitoring capabilities aimed against malware, including ransomware. Your data is safe, secure, and recovery ready. Following the NIST Cybersecurity Framework standards, industry best practices and controls, this multi-layered approach delivers comprehensive data protection.

The quickest and easiest way to get started is in [AWS Marketplace](#), where [Commvault Backup & Recovery](#) is available as an AMI-based image in both usage-based and Bring Your Own License (BYOL) formats. Commvault is committed to assisting you on your cloud journey with consulting, enterprise support, training, and managed services also available via AWS Marketplace.

Intelligent Data Services from Commvault

Commvault delivers its [Intelligent Data Services Platform](#) in AWS Marketplace, closing the business integrity gap and enabling organizations to accelerate business growth. Commvault delivers a flexible, future-proof architecture that provides unprecedented customer choice.

Get started in AWS Marketplace, with the following core Data Management & Protection product(s):

- **Commvault Backup & Recovery** ensures data availability for all workloads across cloud and on-prem environments and delivers reliable, cost-optimized data protection through a single extensible platform.
- **Commvault Disaster Recovery** ensures business continuity and verifiable recoverability across cloud and on-prem environments and delivers replication, disaster recovery, and compliance reporting from a single extensible platform (available as an add-on to Commvault Backup & Recovery).

For more information – see [Commvault solutions in AWS Marketplace](#).

What is AWS Marketplace

AWS Marketplace is a digital catalog that makes it easy for organizations to find, purchase, and deploy third-party software and services within Amazon Web Services (AWS) cloud platform. You can also buy professional services to assist in configuration, deployment, and ongoing support.

AWS Marketplace allows organizations to centralize software and services procurement, perform rapid testing, and accept flexible and customized pricing from their preferred partners. Additionally, centralized governance may be applied on purchasing and deployment practices across the organization.

Learn more at: [What is Amazon Marketplace?](#)

Delivery methods

There are multiple deployment methods offered within AWS Marketplace. Commvault deploys its industry leading Intelligent Data Services platform in the following methods:

- **CloudFormation Stack** – Commvault Backup and Recovery is delivered as a CloudFormation Stack which deploys Commvault on an Amazon EC2 instance with all dependent AWS services created and configured at launch.
- **Amazon Machine Image (AMI)** – Commvault MediaAgents and Access Nodes are delivered as Amazon Machine Images for extended and existing Commvault Backup and Recovery environment.

Pricing Model

There are multiple [Pricing Models](#) available with AWS Marketplace for Infrastructure Software.

All pricing is based on US dollars (USD), Commvault allows purchase from AWS accounts with US-based billing address and payment terms.

Commvault has a single PAID Infrastructure Software product, the **Commvault Backup & Recovery** product uses the following Pricing Model:

- **Usage pricing** leverages the AWS Marketplace Metering service to allow the reporting of consumption to customized dimensions (units), which are invoiced at the end of each calendar month.

See [Commvault usage pricing dimensions](#) for more information.

Professional Services produces are charged upfront immediately to the next monthly invoice.

Commvault also offers several products which leverage by BYOL licensing model.

- **Bring Your Own License (BYOL)** does not incur any software license charges to use, only a consumed AWS services. Commvault offers its Backup & Recovery product as a FREE trial and/or BYOL installation. Commvault also offers its Cloud Access Node as a BYOL component, for extending an existing Commvault environment.

Operating Systems

Commvault is available in several different form-factors and supporting Operating Systems. The following are the available Operating Systems for each production AWS Marketplace. The latest available operating systems are shown.

Product	Operating Systems
Commvault Backup & Recovery	Microsoft Windows Server® 2019 – Data Center Edition Version 1803 (OS Build 17783.2114)
Commvault Backup & Recovery BYOL	Microsoft Windows Server® 2019 – Data Center Edition Version 1803 (OS Build 17783.2114)
Commvault Cloud Access Node BYOL	Red Hat Enterprise Linux 8.5 (Ootpa) Red Hat Enterprise Linux 7.9 (Maipo)
Commvault Cloud Access Node ARM BYOL	Amazon Linux 2

Commvault Solutions in the AWS Marketplace

Commvault Software in the AWS Marketplace

Commvault is committed to providing customers a simple, streamlined deployment of Commvault infrastructure within AWS with all best practices and performance optimizations pre-applied to speed deployment.

Commvault updates and supports these products in accordance with our [Obsolescence Policy](#).

The following [Infrastructure Software](#) products are available in AWS Marketplace.

Product	Pricing model	Purpose
Commvault Backup & Recovery	Usage	Deploys Commvault Backup and Recovery on a single Amazon EC2 instance with required Amazon EBS, IAM, KMS, S3, VPC endpoints, and required licensing. Charges subscription and utility usage to monthly AWS invoice.
Commvault Backup & Recovery BYOL	Bring Your Own License	Deploys Commvault Backup and Recovery on a single Amazon EC2 instance with required Amazon EBS, IAM, KMS, S3, VPC endpoints, and included FREE* 150-day trial license.
Commvault Cloud Access Node BYOL	Bring Your Own License	Deploys a Commvault combined MediaAgent and Access Node for the purpose of performing optimized data movement between protected workloads and Commvault data storage targets (64-bit x86)
Commvault Cloud Access Node ARM BYOL	Bring Your Own License	Deploys a Commvault combined MediaAgent and Access Node for the purpose of performing optimized data movement between protected workloads and Commvault data storage targets (64-bit Arm)

* FREE for 150-days after which a license must be purchased, or AMI-usage based offering must be used.

Commvault services in AWS Marketplace

Commvault provides several Professional Services to assist in the architecture, design, and implementation of Commvault's industry leading Intelligent Data Services platform.

These services may be found in the [Professional Services](#) category within AWS Marketplace.

Contact your Commvault sales representative or email us at aws@commvault.com to discuss your professional services needs.

The following Professional Services products are available.

Product	Pricing model	Purpose
Commvault Technology Consulting	Upfront payment	Architecture, Design, Implementation, Health assessment, Personalization, Data migration, and Residency services.
Commvault Enterprise Support	Upfront payment	Commvault Enterprise Support program with access to dedicated support and technical resources.

Commvault Training	Upfront payment	Education & training services with instructor-led, virtual, and web-based training.
Commvault Managed Services	Upfront payment	Commvault Managed Services for customer owned Commvault deployments.

Getting Started in AWS Marketplace

To get started within AWS Marketplace with Commvault, you will need the following:

- An AWS account with active payment method.
- (Optional) A Private Offer from Commvault, AWS, or Commvault authorized partner for purchase.

Learn more at the [AWS Marketplace – Help](#).

How to create an AWS account

You may create a new AWS Account by following these steps:

1. Navigate to [Amazon Web Services \(AWS\) homepage](#)
2. Click **Sign in the Console** (top-right)
3. Click **Create an AWS Account**
4. Provide **email address, password, and AWS account name**
5. Provide remaining details for **billing and payment**.

For more information see - [How do I create and activate a new AWS account?](#)

Alternatively, see [Finding your AWS account ID](#) to identify your current account details.

How to access AWS Marketplace

AWS Marketplace may be access at: <https://aws.amazon.com/marketplace>

You may search for software and professional services without logging in.

You will need to authenticate with your AWS account to purchase software.

Locating Commvault Software in AWS Marketplace

You can find Commvault in AWS Marketplace within the **Infrastructure Software** and **Professional Services** categories.

Alternatively, if you search for 'Commvault' in [AWS Marketplace](#) you will find all software and services offerings.

Accepting a Private Offer in AWS Marketplace

To accept an [AWS Marketplace Private Offer](#) from Commvault or one of our authorized partners

1. Sign-in into your AWS payer account X (see [Finding your AWS account ID](#)),
2. Navigate to the offer URL which you received.

3. Review pricing and confirm the agreed upon price above across all dimensions.
4. Review End User Agreement.
5. Click **Accept Terms**.

Next Steps

- [Requirements](#)
- [Deploying Commvault in AWS Marketplace](#)
- [Post-deployment tasks](#)
- [Activating your Commvault Support via Amazon Product Connection \(PSC\)](#)
- [Extending your Commvault environment with a MediaAgent and/or Cloud Access Node](#)

Requirements

General requirements

To start using Commvault software in AWS you will require the following:

- An **AWS account** to deploy Commvault software within.
- An existing **Amazon VPC** ([Learn more](#)).
- An existing Amazon VPC Subnet ([Learn more](#)).
- An existing **Amazon EC2 Key Pair** ([Learn more](#)).

System Requirements

Commvault in AWS Marketplace will recommend Amazon EC2 instance sizes based on the Commvault CPU, RAM, and disk space requirements.

The following are the supported instance sizes per Commvault scaling requirements.

Commvault Backup & Recovery

Commvault Backup & Recovery is an all-in-one installation that includes the following packages:

- CommServe
- MediaAgent
- Web Server
- CommCell Console
- Command Center
- Workflow Engine
- Metrics Server
- Index Store
- Index Gateway
- File System Core
- File System
- VSS Provider
- VSS Hardware Provider
- Virtual Server
- Cloud Apps
- IntelliSnap®
- Storage Accelerator
- MongoDB
- Message Queue

The following are the Commvault supported instance sizes for Commvault Backup & Recovery.

Small	Medium	Large	Extra Large
Supports up to 25 servers, or 100 virtual machines, or 200 laptops in a single configuration.	Supports up to 500 servers, or 1000 virtual machines, or 5000 laptops in a single configuration.	Supports up to 2500 servers, or 5000 virtual machines, or 10,000 laptops in a single configuration.	Supports up to 10,000 servers, or 20,000 virtual machines, or 50,000 laptops in a single configuration.
4 CPU cores	8 CPU cores	12 CPU cores	16 CPU cores
24 GB RAM	32 GB RAM	64 GB RAM	128 GB RAM
m5a.2xlarge (default) m5.2xlarge (8 vCPU, 32 GiB)	m5a.2xlarge m5.2xlarge (8 vCPU, 32 GiB)	m5a.4xlarge m5.4xlarge (16 vCPU, 64 GiB)	r5a.4xlarge r5.4xlarge (16 vCPU, 128 GiB)

Commvault also supports t3a.xlarge, t3a.2xlarge for dev/test or POC initiatives.

Cloud Access Node – Snapshot Only

Commvault Cloud Access Node is a data movement instance that includes the following packages:

- Virtual Server
- MediaAgent
- File System Core
- File System
- Cloud Apps
- IntelliSnap®

The following are the Commvault supported instance sizes for Cloud Access Nodes used exclusively for orchestrating snapshot backup and replication.

Cloud Access Node – Snapshot only
Supports snapshot creation and replication to alternate region(s) or accounts for Amazon EC2 and Amazon RDS data management. Scale horizontally when backup cannot be completed within designated protection window.
2 CPU cores
4 GB RAM
c6g.large (default, 64-bit Arm) c5.large (default, 64-bit x86) (2 vCPU, 4 GiB)

Cloud Access Node – Snapshot and Streaming

Commvault Cloud Access Node is a data movement instance that includes the following packages:

- Virtual Server
- File System Core
- Cloud Apps
- MediaAgent
- File System
- IntelliSnap®

The following are the Commvault supported instance sizes for Cloud Access Nodes used for snapshot and streaming based backup and recovery (including the hosting of Deduplication Databases).

Extra-Small	Small	Medium	Large	Extra-Large
Protects 5-10 Front End Terabytes (FETB) of Amazon client data.	Protects 10-25 Front End Terabytes (FETB) of Amazon client data.	Protects 25-50 Front End Terabytes (FETB) of Amazon client data.	Protects 50-100 Front End Terabytes (FETB) of Amazon client data.	Protects 90-120 Front End Terabytes (FETB) of Amazon client data.
r6g.large (64-bit Arm)	r6g.xlarge	m5a.2xlarge	m5a.4xlarge	r6g.4xlarge
r5a.large (64-bit, x86)	r5a.xlarge	r6g.2xlarge	r6g.4xlarge	r5a.4xlarge
2 CPU cores	4 CPU cores	8 CPU cores	12 CPU cores	16 CPU cores
16 GB RAM	24 GB RAM	32 GB RAM	64 GB RAM	128 GB RAM

AWS Identity and Access Management Requirements

Commvault automatically provisions the AWS IAM Role and required inline policies for data management and protection as part of AWS CloudFormation deployment.

For more information on the required [AWS User Permissions](#), see [Amazon Web Services User Permissions for Backups and Restores](#).

The follows are the AWS IAM inline policies attached to the CommvaultBackupAndRecovery IAM Role created via AWS CloudFormation. The role has a trust relationship on ec2.amazonaws.com and is attached to the Commvault CommServe® server during deployment.

IAM Inline Policy	Policy Source
CloudWatchAgentServerPolicy (AWS managed policy)	Used by Commvault Backup & Recovery instances to send disk space consumption to the AWS CloudWatch service for alarming and automated action.
AmazonSSMManagedInstanceCore (AWS managed policy)	Used by Commvault Backup & Recovery auto-scaling for amazon access nodes and agentless file recovery .
Commvault_AmazonDocDBProtection	Used for data management and protection of Amazon DocumentDB tables. amazon_documentdb_backup_restore_permissions.json

IAM Inline Policy	Policy Source
Commvault_AmazonDynamoDBProtection	Used for data management and protection of Amazon DynamoDB instances. AWS_DynamoDB_permissions.json
Commvault_AmazonEC2Protection	Used for data management and protection of Amazon EC2 instances and attached Amazon EBS volumes, both within AWS Cloud and on AWS Outposts. amazon_restricted_role_permissions.json
Commvault_AmazonImportExport	Used for performing VM conversion from on-premises VM backups to Amazon EC2 instances, using Amazon Import/Export service. See VM Conversion Using the Import Method trust-policy.json role-policy.json
Commvault_AmazonMarketplaceMetering	See IAM policy for AMI products .
Commvault_AmazonOutpostsS3Protection	Used for performing data management and protection of Amazon S3 object data located on AWS Outposts. See Protecting S3 Data in AWS Outposts amazon_s3_on_outposts_permissions.json
Commvault_AmazonRDSProtection	Used for performing data management and protection of Amazon Relational Database Service (RDS) databases (including Amazon Aurora) located on AWS cloud and AWS Outposts. amazon_rds_backup_restore_permissions.json
Commvault_AmazonRedshiftProtection	Used to perform data management and protection of Amazon Redshift instances. amazon_redshift_backup_restore_permissions.json
Commvault_AmazonS3Protection	Used to perform data management to Amazon S3 buckets when created within Commvault as Commvault Cloud libraries. amazon_s3_EC2_IAM_role_01.json amazon_s3_EC2_IAM_role_02.json amazon_s3_EC2_IAM_role_03.json
Commvault_IntelliSnapDBFSProtection	Used to perform data management and protection of traditional applications, file systems, and databases located on Amazon EC2 instances. Provides the ability to perform application consistent snapshot protection. amazon_DB_FS_backup_restore_permissions.json

IAM Inline Policy	Policy Source
Commvault_VMConversion	Used to perform Commvault optimized VM conversion from on-premises or non-AWS cloud backups to native Amazon EC2 instances. See Cross Hypervisor Restores (VM Conversion) amazon_permission_conversion.json

For more information on how Commvault uses each IAM policy – see [Amazon Web Services Permission Usage](#)

Service endpoints

Commvault integrates natively with a number global and regional services to provide industry leading Intelligent Data Services. The following service endpoints must be accessible from Commvault infrastructure via a VPC PrivateLink endpoint or Internet Gateway (IGW), NAT Gateway or HTTP proxy.

Learn more at [AWS service endpoints](#).

Regional endpoints

Service endpoint	Purpose
cloudhsmv2.{region}.amazonaws.com	Used when leveraging AWS CloudHSM to provide cryptographic operations to AWS workloads. Commvault supports KMIP compliant key management services (SafeNet, Vormetric) which support CloudHSM .
documentdb.{region}.amazonaws.com	Used to perform cloud-native snapshot-based data management and protection for Amazon DocumentDB NoSQL database clusters.
dynamodb.{region}.amazonaws.com	Used to perform streaming data management and protection for Amazon DynamoDB tables across multiple accounts and regions.
ec2.{region}.amazonaws.com	Used to perform data management and protection for Amazon EC2 instances. Also used to provide Amazon Virtual Private Cloud (VPC) discovery.
ec2message.{region}.amazonaws.com (for SSM)*	Used with automatic scaling for amazon access nodes, to dynamically provision Commvault EC2 infrastructure during backup and recovery operations.
ebs.{region}.amazonaws.com	Used to perform data management and protection for Amazon Elastic Block Store (EBS) volumes.
glacier.{region}.amazonaws.com	Used to perform data management to and from Amazon S3 Glacier services. Commvault uses Amazon S3 Glacier to store backup and archival data in Commvault combined storage tier libraries.
kms.{region}.amazonaws.com	Used to perform secure data management and protection for Amazon services that contain data encrypted with AWS Key Management Service (AWS) encryption keys.

monitoring.{region}.amazonaws.com	Used to register AWS CloudWatch alarms for monitoring Commvault Backup & Recovery accessibility, responsiveness, and disk space remains within recommended thresholds.
outposts.{region}.amazonaws.com	Used to perform data management and protection for Amazon Outposts-based EC2, EBS, EKS, RDS, and S3 data.
rds.{region}.amazonaws.com	Used to perform data management and protection for Amazon Aurora (MySQL, PostgreSQL), Amazon Relational Database Services (RDS).
redshift.{region}.amazonaws.com	Used to perform data management and protection for Amazon Redshift clusters.
s3.{region}.amazonaws.com	Used to perform data management and protection for Amazon S3 data, and to store and replicate backup data into Amazon S3, S3 Glacier, and S3 Glacier Deep Archive cloud libraries.
snowball.{region}.amazonaws.com	Used to perform data management to and from AWS Snow family devices. AWS Snow family allows the offline migration of data into and out of AWS Cloud.
sts.{region}.amazonaws.com	Used to obtain temporary credentials from the AWS Secure Token Service (STS) , which are used in the data management and protection of AWS services.
ssm.{region}.amazonaws.com*	Used to register Commvault access nodes created with automatic scaling for amazon access nodes , and to provide agentless file recovery into Amazon EC2 instances. NOTE: Both global and regional endpoint access is required.
ssmmessages.{region}.amazonaws.com (for SSM)*	Used to register Commvault access nodes created with automatic scaling for amazon access nodes , and to provide agentless file recovery into Amazon EC2 instances.

Global endpoints

Column head	Column head
iam.amazonaws.com	Used to secure and provide access to AWS services.
importexport.amazonaws.com	Used to perform cross hypervisor restores (VM Conversion) which leverage the AWS Import/Export service to convert on-premises VM backups to Amazon EC2 instances.
sts.amazonaws.com	Used to obtain temporary credentials from the AWS Secure Token Service (STS) , which are used in the data management and protection of AWS services. NOTE: Both global and regional endpoint access is required.

AMI usage requirements

The following section below details the requirements for Commvault Backup & Recovery to be able to **meter** your software consumption to the AWS Marketplace Metering Service.

IF your chosen subnet has internet access, then access to the **AWS Marketplace Metering Service** will simply function. If there are firewalls or other network controls in place – you will need to extend them to the endpoint listed below.

Your Commvault Backup & Recovery instance will be provided with a Commvault_AmazonMarketplaceMetering **inline IAM policy** pre-created and attached to your instance. The information here is provided if the original IAM Role and/or policy is removed.

Service Endpoints

If utilizing the Commvault Backup & Recovery PAID product from AWS Marketplace, your Commvault CommServe® server will require access to the **AWS Marketplace Metering Service**:

- metering.marketplace.{region}.amazonaws.com

See [AWS Marketplace endpoints and quotas](#) for more information.

IAM policy for AMI products

For Commvault to be able to send usage information to the AWS Marketplace Metering Service, the following IAM policy must be attached to the Commvault CommServe® server.

This policy is created by the Commvault CloudFormationStack associated with the Commvault Backup & Recovery product(s) as an [inline policy](#) on the CommvaultBackupAndRecovery IAM Role

Policy name: Commvault_AmazonMarketplaceMetering

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": "aws-marketplace:MeterUsage",
      "Resource": "*",
      "Effect": "Allow"
    }
  ]
}
```

Deploying Commvault in AWS Marketplace

Deploying Commvault Backup & Recovery BYOL

To deploy Commvault Backup & Recovery Bring Your Own License (BYOL) edition from the AWS Marketplace, perform the following steps.

Deploying Commvault Backup and Recovery BYOL CloudFormation Stack

1. Login to the [AWS Marketplace](#)

2. Search for “Commvault” or go to [Commvault on AWS Marketplace](#)
3. Select the **Commvault Backup & Recovery BYOL** product.
4. Click **Continue to Subscribe** button.
5. Review the **End User License Agreement (EULA)**, **AWS Privacy Notice**, and **AWS Customer Agreement**.
6. Review **Pricing Information** (NOTE: BYOL product has not pricing it is FREE for 150 days).
7. Click **Accept Terms** (wait for subscription to be established)
8. Click **Continue to Configuration** button.
9. Select **Commvault Backup & Recovery: BYOL Deployment** as the delivery method.
10. (Optional) Select the preferred **Software Version** (latest will be selected)
11. (Optional) Review deployment by clicking **Learn more**
12. Select **Region** for deployment
13. (Optional) Review the release notes, by clicking **Release notes**.
14. Click **Continue to Launch**.
15. Click **Usage Instructions** for details to perform after successful deployment
16. Select **Launch CloudFormation** as the launch action
17. Select **Launch** button
18. Click **Next** to Specify CloudFormation Stack Details
19. Complete the CloudFormation parameters, click **Next** (see
20. Click **Next** to move to Review
21. Click **I acknowledge that AWS CloudFormation might create IAM resources**
22. Click **Create Stack**

Continue with [post-deployment tasks](#) to complete initial configuration of Commvault Backup & Recovery.

AMI-based deployment

It is possible to deploy Commvault Backup & Recovery as an Amazon Machine Image (AMI) deployment only. This method will not pre-configure the required Amazon Identity & Access Management (IAM) roles and instance profiles required to perform data management and protection.

Commvault does not recommend this method, see [Deploying Commvault Backup & Recovery BYOL](#) for instructions on deploying using AWS CloudFormation.

To deploy an AMI image only:

1. Login to **AWS Console** <https://signin.aws.amazon.com/console>
2. Navigate to the EC2 Dashboard <https://console.aws.amazon.com/ec2/v2/home?region=us-east-1>
3. Click **Launch Instances** ▼
4. Search for **Commvault Backup & Recovery BYOL**
5. Click **AWS Marketplace** (left)
6. Click **Select** on the located AMI image

7. Click **Continue**
8. Choose **Instance Type**, select **Next**
9. Configure **Instance Details**, select **Next**
10. Configure/review **Storage**, select **Next**
11. Add **Tags**, select **Next**
12. Select **Create a new security group**, review settings, select **Review and Launch**
13. Click **Launch**

Continue with [post-deployment tasks](#) to complete initial configuration of Commvault Backup & Recovery.

Related Topics

[Deploying a Commvault Access Node from AWS Marketplace](#)

Deploying Commvault Backup & Recovery

To deploy Commvault Backup & Recovery **AMI usage** edition from the AWS Marketplace, you can take two (2) paths:

- [Accept the AWS Marketplace Public Offer](#) (default pricing, no discount)
- [Accept an AWS Marketplace Private Offer](#) (custom pricing, potential discounting)

Select the method you will be using and following the steps, once complete you can move onto deploying Commvault Backup & Recovery.

Accepting the AWS Marketplace Public Offer

Use this method to purchase Commvault Backup & Recovery from the public AWS Marketplace.

1. Login to the AWS Marketplace <https://aws.amazon.com/marketplace>
2. Search for “Commvault” or go to [Commvault on AWS Marketplace](#)
3. Select the **Commvault Backup & Recovery** product.
WARNING: Ensure you do not select the BYOL image.
4. Click **Continue to Subscribe** button.
5. Review the **End User License Agreement (EULA)**, **AWS Privacy Notice**, and **AWS Customer Agreement**.
6. Review **Pricing Information** (**NOTE:** Pricing is dependent on the public or [private offer](#) that your accepted)
7. Click **Accept Terms** (wait for subscription to be established)
8. Click **Continue to Configuration** button.

Accepting an AWS Marketplace Private Offer

Before you can deploy Commvault Backup & Recovery, you will need an active AWS Marketplace subscription. If you have received a [private offer](#) from Commvault or one of our authorized partners, perform the following steps to accept the offer and establish a Marketplace subscription.

1. Login to the AWS Marketplace <https://aws.amazon.com/marketplace>
2. Open the **Offer URL** provided by Commvault or an authorized Commvault partner.
3. Review the **End User License Agreement (EULA)**, **AWS Privacy Notice**, and **AWS Customer Agreement**.

4. Review **Pricing Information**
5. Click **Accept Terms** (subscription will now be established)
6. Click **I'll do this later** to provide Product Support Connection (PSC) details at a later time (See [Activation your Commvault Support via Amazon Product Support Connection](#))

NOTE: Commvault recommends activating PSC after your subscription has been successfully created and shows an **effective date** (see below)

Product	Effective date	Expiration date	Action
Commvault Backup & Recovery	9/6/2021	N/A	▼ Show Details

You may now continue to deploy Commvault by clicking **Continue to Configuration**.

Deploying Commvault Backup & Recovery CloudFormation Stack

To deploy Commvault Backup & Recovery using a previously established subscription, you may click **Continue to Configure** after establishing the subscription or follow the steps below.

1. Login to [AWS Console](#)
2. Search and select [AWS Marketplace Subscriptions](#)
3. Select **Commvault Backup & Recovery** (click title or click **Manage** button)
4. Open **Actions ▼** menu, select **Launch CloudFormation Stack**
5. Select **Commvault Backup & Recovery: Standard / Custom / Additional Deployment** as the delivery method. (See [Commvault and AWS CloudFormation](#) for details on which option to pick)
6. (Optional) Select the preferred **Software Version** (latest will be selected)
7. (Optional) Review deployment by clicking **Learn more**
8. Select **Region** for deployment
9. (Optional) Review the release notes, by clicking **Release notes**.
10. Click **Continue to Launch**.
11. Click **Usage Instructions** for details to perform after successful deployment
12. Select **Launch CloudFormation** as the launch action
13. Select **Launch** button
14. Click **Next** to Specify CloudFormation Stack Details
15. Complete the CloudFormation parameters, click **Next** (See [Commvault and AWS CloudFormation](#) for details on how to answer the CloudFormation questions)
16. Click **Next** to move to Review
17. Click **I acknowledge that AWS CloudFormation might create IAM resources**
18. Click **Create Stack**

Continue with [post-deployment tasks](#) to complete initial configuration of Commvault Backup & Recovery.

AMI-based deployment

Deployment of the **Commvault Backup & Recovery** paid AMI-usage product is not supported as a direct AMI deployment. Please complete the [Deploying Commvault Backup & Recovery CloudFormation Stack](#) procedure (above) to deploy using AWS CloudFormation.

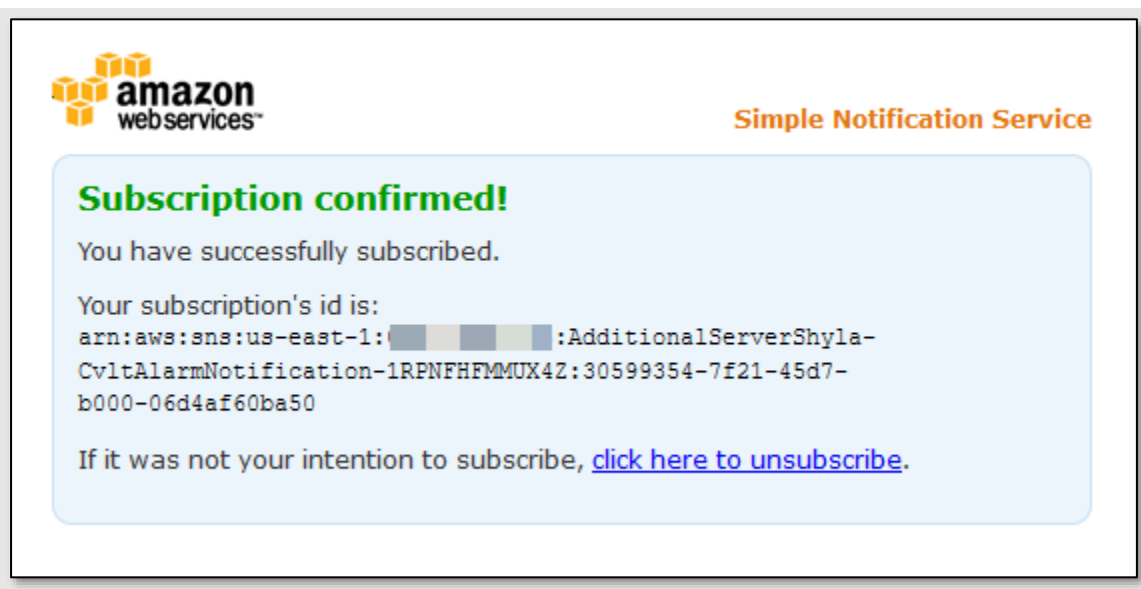
Activating AWS CloudWatch DiskSpace notification

During AWS CloudFormation deployment, a new Simple Notification Service (SNS) Topic will be created to receive notifications from CloudWatch and forward to the Commvault administrator email address supplied as a CloudFormation parameter.

To start receiving email alerts you will need to **accept** the SNS subscription. To activate the disk space alarm notification, perform the following:

1. Open the email inbox or distribution list supplied during AWS CloudFormation setup.
2. Look for an email from **AWS Notifications** no-reply@sns.amazonaws.com
Subject will be: AWS Notification - Subscription Confirmation
3. Click the **Confirm subscription** link in the email.

You will receive a confirmation in the browser window (see below)



Post-deployment tasks

Continue with [post-deployment tasks](#) to complete initial configuration of Commvault Backup & Recovery.

Related Topics

- [AWS CloudFormation FAQs](#)

Deploying Commvault Cloud Access Node BYOL

To deploy Commvault Cloud Access Node Bring Your Own License (BYOL) edition from the AWS Marketplace, perform the following steps.

Procedure

1. Login to [AWS Console](#)
2. Navigate to the [EC2 Dashboard](#)
3. Click **Launch Instances** ▼
4. Search for **Commvault Cloud Access Node** or **Commvault Cloud Access Node ARM** (AWS Graviton2 instance type)
5. Click **AWS Marketplace** (left)
6. Click **Select** on the located AMI image
7. Click **Continue**
8. Choose **Instance Type**, select **Next**
9. Configure **Instance Details**, select **Next**
10. Configure/review **Storage**, select **Next**
11. Add **Tags**, select **Next**
12. Select **Create a new security group**, review settings, select **Review and Launch**
13. Click **Launch**

Following the procedure in [Deploying a Commvault Linux MediaAgent from AWS](#) to register the new Access Node with your Commvault Backup & Recovery instance.

Post deployment tasks

After your Commvault Backup & Recovery instance is deployment and running, you can login and perform initial setup to start protecting your AWS workloads.

Obtaining your login credentials

To obtain your login credentials for your Commvault Backup & Recovery instance, perform the following:

1. Login to **AWS Console** <https://signin.aws.amazon.com/console>
2. Navigate to the EC2 Dashboard <https://console.aws.amazon.com/ec2/v2/home?region=us-east-1>
3. Click the **instance** you would like to obtain credentials
4. Right-click, **Security, Get windows password**
5. Click **Browse** to locate your Amazon EC2 key pair (Key pair name will be listed above the button)
6. Click **Decrypt password**
7. Copy the **Private IP Address, User name, and Password**

See [How do I retrieve my Windows administrator password after launching an instance?](#) for more information.

You can now use this information to access your host via Remote Desktop Protocol (RDP).

Creating your admin account

Upon first login to your Commvault Backup & Recovery instance, a Powershell script will pre-configure your Commvault software and then launch Chrome browser to create your initial **administrator account**.

Procedure

1. Log on to the Commvault Backup & Recovery instance as **Administrator**
2. When the **Create new account** window opens, enter your **email address** and **password** (x2)
3. Click **Create Account**
4. Browser will refresh and display the Commvault Command Center™ login window.

Continue onto **Completing Core Setup** (below) to complete initial setup.

Completing Core Setup

Before Commvault can start protecting your AWS services, you must configure a Commvault Cloud Library to store backup data, and an associated Server plan which specifies the frequency and retention of your backup data.

For more information, see [Complete the Core Setup Wizard](#)

Retrieving your Amazon S3 bucket name

Before starting **core setup**, you will want to retrieve the Amazon S3 Standard bucket pre-created during AWS CloudFormation deployment. Follow these instructions to locate your bucket name:

1. Login to **AWS Console** <https://signin.aws.amazon.com/console>
2. Search for **CloudFormation**, select it <https://console.aws.amazon.com/cloudformation/home?region=us-east-1>
3. Locate your Stack, click the **Stack name**
4. Click the **Outputs** tab
5. Note the **Vault** of the **CvltCloudLibraryBucketName**

Procedure

Complete the following procedure to prepare your Commvault Backup & Recovery instance for data management and protection operations.

1. Login to Command Center as **admin**, with your supplied password.
2. Click **Let's get started >**
3. Within **Add Storage**, click **Cloud**
4. Enter a **Name** for the Commvault Cloud Library
5. Select Type = **Amazon S3**
6. Leave the MediaAgent (default)
7. Within Service Host, replace [region] with the region for your instance (for example, s3.us-east-1.amazonaws.com)
8. Select Authentication = **AWS IAM role policy**
9. Set Bucket = <bucket name retrieved from [CloudFormation Outputs](#)>
10. Set the Storage class = **Standard – Infrequent Access** if you will retain backups for at least 30 days.
11. In Deduplication DB Location, click **Browse** icon
12. Click **DDB1**
13. Click **New Folder**
14. Enter a folder name, click **Add**, click **Save**
15. Click **Save** to create Cloud Library
16. In **Create server plan**, click **Save** (to save with defaults)

Other post deployment tasks

Commvault recommends performing the following additional post deployment tasks in alignment with your organizational security policy:

- Enable Windows Update automatic patch download and install
- Configure Commvault [recommend anti-virus exclusions](#)
- Enable the Object Storage protection menu, if protecting Amazon S3.
 - Click **Guided Setup**
 - Click **Protect, more** ○Click **Object storage**

- Click **Mark this setup as complete**
 - *Browser will refresh and Protect > Object Storage menu will now be available.*
- Enable the Kubernetes protection menu, if protecting Amazon EKS
 - Open **Manage > Customization > Navigation**
 - Expand **Protect**, select **Kubernetes** for all users
 - Click **Save**, click **Yes** to confirm
 - **Logout** and **Login** into Command Center
 - *Protect > Kubernetes menu will now be available.*
- [Add an Amazon Access Node](#) to perform File Recovery Enabler tasks for granular Linux file & folder recovery

Activating your Commvault Support via Amazon Product Connection (PSC)

If you have purchased Commvault Backup & Recovery from the AWS Marketplace, your subscription includes Commvault [Premium Support](#) services.

Once you have deployed your first Commvault Backup & Recovery instance, you should activate your support services for ongoing access to updates, knowledge base articles and chat / telephone support services.

To activate your Premium Support services, perform the following:

1. Login to AWS Marketplace

To get started – go to aws.amazon.com/marketplace and ensure you are logged into the AWS account that purchased Commvault Backup & Recovery.

2. Open Your Marketplace Software

Click your **username** ▼ (top-right) and select **Your Marketplace Software** to open your active AWS Marketplace subscriptions

3. Open Product Support Connection

In order for Commvault to activate your support services, we need your **contact information**.

Click **Product Support Connection** to provide the contact details (Name, Telephone, Email) for up to five (5) support representatives responsible for supporting Commvault Backup & Recovery in your organization.

When you open Product Support Connection for the first time, it will likely indicate you have not shared your contact information. This is default behavior within AWS Marketplace, you must **opt-in** to share your contact information.

4. Provide contact details

Click the **Share your contact details** for a product and select your subscription. Click **Continue** to enter and share your contact details.

All fields are **mandatory**. Accept the permission to share agreement checkbox and click **Register & Close**.

You may click **Register & Add Another** to add additional support contacts up to a maximum of five (5).

NOTE: Commvault will send login details to access ma.commvault.com to the **first registered user** only.

You will receive confirmation of successful sharing. Commvault will receive these details and activate your support account within **2 business days**.

NOTE: If you do not receive login details please contact Commvault Toll Free: +1 877-780-3077 (**Worldwide numbers >**)

Where to go next

You will want to keep your Commvault system patched and ready to protect all your new Amazon services, so head over to [ma.commvault.com >](https://ma.commvault.com) and optionally download additional free software add-ons (200+ reports, workflows, and automation to make your life easier).

Other Operations

Configuring AWS backups

After initial deployment, you will want to get started protecting your Amazon services. Following the instructions below to configure protection activities for your AWS services.

Amazon EC2 protection

Getting started protecting Amazon EC2 instances is a simple three step process:

1. [Adding an Amazon Hypervisor](#)
2. [Adding a VM Group for Amazon](#)
3. [Backing Up an Amazon VM Group or Instance On Demand](#)

Commvault utilizes the Amazon Direct APIs to perform cloud-native EC2 and EBS protection – see [Enabling or Disabling Changed Block Tracking for Backups](#) for details (enabled by default).

Learn more at [Virtualization & Cloud – Amazon](#)

Amazon EFS protection

Commvault protects Amazon Elastic File System (EFS) exports using full, differentials, incremental, and synthetic full streaming backups. Get started protecting your EFS file systems with this simple process:

1. Ensure you have a **Commvault Cloud Access Node BYOL** or **Commvault Cloud Access Node ARM BYOL**
2. Click **Protect > File Servers**
3. Click **Add Server** (top right)
4. Click **NAS**
5. Enter a **Name**
6. Enter the **Fully Qualified Host Name** of the EFS endpoint (for example, fs-6ed41f15.efs.us-east-2.amazonaws.com)
7. Select a **Plan**
8. Open **Network Share Configuration**
9. Enable the **NFS** toggle
10. Select at least one **Access Node**, click **Ok**
11. Leave the content set as **All NFS Exports** -or-
Click **Edit**, enter a fully qualified path with export, click **+** sign (for example, fs-6ed41f15.efs.us-east-2.amazonaws.com:/)
12. Click **Save**
13. Click **Save**
14. Click **NFS** in the Protocols section (bottom)
15. Click **Back up**, select Full / Incremental, Click **Ok**

For more details, see [AWS EFS \(Amazon Elastic File System\)](#)

Caveats

When adding content to protect, the **Browse** button cannot be utilized. Please review file systems and folders to protect on the Unix host, and then add accordingly.

Amazon EKS protection

Protecting your modern containerized applications being managed by Kubernetes or Amazon EKS is simple with Commvault. Amazon EKS, EKS-D and EKS on Outposts are all fully supported for backup ,recovery, and data migration activities. Follow these steps to get started:

1. (Optional) Complete [Kubernetes Guided Setup](#) to activate the Kubernetes protect menu
2. [Create a Service Account for Kubernetes](#)
3. [Add the Kubernetes Cluster](#)
4. [Create an Application Group of the Content to Back Up](#)
5. [Perform a Test Backup and Restore of the Kubernetes Application](#)

For more details, see [Kubernetes](#)

NOTE: Commvault recommends using the [Amazon EBS CSI driver](#) to orchestrate the creation of Amazon EBS snapshots for Kubernetes backup & recovery.

Amazon FSx for Windows protection

Commvault protects Amazon FSx for Windows shares using full, differentials, incremental, and synthetic full streaming backups. Get started protecting your FSx file systems with this simple process:

1. Click **Protect > File Servers**
2. Click **Add Server** (top right)
3. Click **NAS**
4. Enter a **Name**
5. Enter the **DNS Name** of the FSx file system
(for example, amznfsxooijnmo4.mkt.commvault.com)
6. Select a **Plan**
7. Open **Network Share Configuration**
8. Enable the **NFS** toggle
9. Select at least one **Access Node**, click **Ok**
10. On CIFS credentials, click **Edit**
11. Enter a Domain **Username** (for example, DOMAIN\fs-admin)
12. Enter a Domain **Password**, click **OK** to save
13. Leave the content set as **All CIFS Shares** -or-
Click **Edit**, Click **Browse**, Click and **Access Node**, click **OK**
14. Expand the **Path** and select the **shares**, and **folders** you would like to protect
15. Click **Save**
16. Click **Save**
17. Click **Save** to add the FSx SMB share
18. Click **CIFS** in the Protocols section (bottom)
19. Click **Back up**, select Full / Incremental, Click **Ok**

For more details, see [Amazon FSx for Windows File Server](#)

NOTE: Backup performance will be directly impacted by the **Storage type** and **Throughput capacity** configured on the FSx file system. Throughput capacity may be dynamically updated, see [Managing throughput capacity](#).

Amazon DocumentDB protection

Commvault protects Amazon DocumentDB clusters across multiple accounts and regions. Commvault integrates with AWS native snapshots to protect Amazon DocumentDB clusters. Follow these steps to get started protecting your Amazon DocumentDB clusters:

1. [Creating a Cloud Database Instance for Amazon DocumentDB](#)
2. [Creating a Cluster Group to Back Up Specific DocumentDB Clusters](#)
3. [Backing Up a DocumentDB Cluster Group](#)

For more information, see [Amazon DocumentDB](#).

Amazon DynamoDB protection

Commvault protects Amazon DynamoDB tables across multiple accounts and regions. Commvault integrates with the DynamoDB data access APIs for full and incremental backups. Follow these steps to get started protecting your Amazon DynamoDB tables:

1. [Creating a Cloud Database for Amazon DynamoDB](#)
2. [Creating a Table Group for a Set of DynamoDB Tables](#)
3. [Performing a Backup of a DynamoDB Database Instance](#)

You may optionally perform these steps to optimize the performance of DynamoDB backups, [Optimizing the Backup Performance for a DynamoDB Table Group](#).

For more information, see [Amazon DynamoDB](#).

AWS Outposts protection

You can use Commvault to protect EC2, EBS, EKS, RDS, and S3 data located on AWS Outposts. Follow these steps to protect your AWS Outposts workloads:

1. [Deploy a Commvault Cloud Access Node](#) into the Outposts to access and optionally storage data locally.
2. Activate protection for each of your workload types within the Outposts – [EC2](#), [EKS](#), [RDS](#), and [S3](#).
3. (Optional) [Configure Replication between AWS Outposts and AWS cloud](#).

For more information, see [AWS Outposts](#).

Amazon RDS protection

You can use Commvault software to protect Amazon RDS instances across multiple accounts and regions. Commvault integrates with AWS native snapshots to protect Amazon RDS instances. Commvault can also connect to the database directly using database native dump/export tools to create logical dump of the database outside the Amazon RDS service.

Snapshot protection

1. [Creating a Cloud Database Instance for Amazon RDS](#)
2. [Creating an Instance Group to Back Up Specific Amazon RDS Instances](#)
3. (Optional) [Enabling Cross-Account Sharing of an Amazon RDS Snapshot Copy to the Same or a Different Region](#)
4. (Optional) [Enabling Cross-Account Copying of an Amazon RDS Snapshot Copy to the Same or a Different Region](#)
5. [Backing Up an Amazon RDS Instance Group](#)

For more information, see [Amazon RDS Snapshot Backup](#).

Dump/export protection

The processes for performing a dump/export-based backup vary greatly between database vendors. Commvault supports dump/export backups of the following database types:

- [Aurora MySQL](#)
- [Aurora PostgreSQL](#)
- [RDS for MariaDB](#)
- [RDS for MySQL](#)
- [RDS for PostgreSQL](#)
- [Amazon RDS for SQL Server](#)
- [Amazon RDS for Oracle](#)

Follow the link to the database you are looking to backup.

For more information, see [Amazon RDS Protection Using Native Database Export or Dump Utility](#).

Amazon Redshift protection

Commvault software protects Amazon Redshift clusters across multiple accounts and regions. Commvault integrates with AWS native snapshots to protect Amazon Redshift clusters. To get started protecting your Redshift clusters, perform the following:

1. [Creating a Cloud Database Instance for Amazon Redshift](#)
2. [Creating a Cluster Group to Back Up Specific Redshift Clusters](#)
3. [Backing Up a Redshift Cluster Group](#)

For more information, see [Amazon Redshift](#).

Amazon S3 protection

You can use the Commvault software to back up and restore Amazon Simple Storage Service (S3). Coupled with Commvault deduplication, compression, and encryption this allows the protection, replication, and storing of Amazon S3 backups at reduced cost. Commvault reduces your S3 storage and VPC egress fees (when replicating cross region). To get started protecting Amazon S3, follow these steps:

1. [Add the Amazon Simple S3 Object Storage Repository with an IAM Role Policy](#)
2. [Add a Content Group to the Amazon S3 Object Storage Repository](#)
3. [Perform a Test Backup and Restore of the Amazon S3 Object Storage Repository](#)

For more information, see [Amazon S3 \(Simple Storage Service\)](#).

Performing AWS restores

When disaster hits, you need your data and applications backup – fast! Use this section to find the recovery process for each of your protected Amazon services.

Restoring Amazon EC2 data

Restoring Amazon EFS data

Commvault supports a multitude of recovery use-cases based on the scope of the Amazon EC2 data loss event. See below for the process for each restore type:

- [Restoring Guest Files and Folders for Amazon](#)
- (Optional) [Configuring Agentless File Recovery for Amazon](#)
- [Attaching a Volume to an Existing Amazon Instance](#)
- [Attaching a Volume to a New Amazon Instance](#)
- [Restoring Full Instances for Amazon](#)

See [Restores](#) and [Other Operations](#) for additional information.

Restoring Amazon EKS data

Commvault supports a multitude of recovery use-cases based on the scope of the Amazon EKS, EKS-D, Red Hat OpenShift on AWS data loss event. See below for the process for each restore type:

- [Restores of Kubernetes Persistent Volumes, Files and Folders](#)
- [Restores of Kubernetes Application Manifests](#)
- [Restores of Kubernetes Applications](#)

See [Restores](#) for additional information.

Restoring Amazon FSx for Windows data

Refer to [Restoring NAS File Server Data](#) for the process to restore FSX for Windows SMB data.

Data may be restored by to the original location, or to an alternate location access by Commvault.

Restoring Amazon DocumentDB data

Commvault can restore an entire Amazon DocumentDB cluster to a new cluster with specified chosen availability zone, and with a specific node type selected during creation.

See [Restoring a DocumentDB Cluster](#) for the detailed procedure.

Restoring Amazon DynamoDB data

Commvault can restore your Amazon DynamoDB data at an individual table, multiple tables, or all tables in a region level. Additionally, restores can span accounts, regions and change table names for seeding new development initiatives. Follow these steps for performing DynamoDB restores:

[Restoring Tables for DynamoDB](#)

Restoring Amazon Outposts data

You can use Commvault to restore EC2, EBS, EKS, RDS, and S3 data located on AWS Outposts or from the region. Follow these steps to restore your AWS Outposts workloads:

1. [Deploy a Commvault Cloud Access Node](#) into the Outposts to access and optionally storage data locally.
2. Utilize restore procedure relevant to each workload type protected – [EC2](#), [EKS](#), [RDS](#), and [S3](#).
3. (Optional) [Configure Replication between AWS Outposts and AWS cloud](#).

For more information, see [AWS Outposts](#).

Restoring Amazon RDS data

You can restore an Amazon RDS instance (snapshot backup) to a selected target availability zone and change the node type of the instance during the restore. Additionally, you can restore Amazon RDS (dump/exports) to existing or new database instances located on Amazon EC2, AWS Outposts or back on-premises.

Snapshot restores

To restore an instance from Amazon RDS snapshot, see [Restoring an Amazon RDS Instance](#).

Dump/export restores

The processes for performing a dump/export-based restore vary greatly between database vendors. Commvault supports dump/export restores of the following database types:

- [Aurora MySQL](#)
- [Aurora PostgreSQL](#)
- [RDS for MariaDB](#)
- [RDS for MySQL](#)
- [RDS for PostgreSQL](#)
- [Amazon RDS for SQL Server](#)
- [Amazon RDS for Oracle](#)

Follow the link to the database you are looking to backup.

For more information, see [Amazon RDS Protection Using Native Database Export or Dump Utility](#).

Restoring Amazon Redshift data

You can restore a Redshift cluster to a selected target availability zone and change the node type of the cluster during the restore.

See [Restoring a Redshift Cluster](#) for the detailed process for recovery.

Restoring Amazon S3 data

You can restore Amazon S3 data to its original location, to any of the [supported cloud storage systems](#), and to disk. You can restore data, along with the metadata and ACLs to the original bucket, or to a different bucket in the same cloud.

See [Restores for Amazon S3](#) for the process to restore to original or new location.

Disaster Recovery for Amazon EC2

To protect your data during a potential disaster or planned downtime, you can copy and sync data to multiple locations using the following Commvault replication features. Commvault Backup & Recovery in AWS Marketplace supports **Virtual Machine Replication** to provide replication, failover, failback for VMs between cloud regions or on-premises and cloud.

Configuring periodic replication

You can replicate a VM Group by creating a recovery target and replication group. VMs are backed up and replicated according to the settings in the replication group. Commvault automatically created Amazon EC2 instances in the recovery target region/subnet as part of the periodic replication process.

To configure replication, see [Creating a Replication Group from a VM Group](#).

Monitoring AWS Disaster Recovery replication status

Use the Replication monitor to view sync status information for periodic replication.

To access the **Replication monitor** within Commvault Command Center

1. From the navigation pane, go to **Disaster recovery > Replication Monitor**.
The **Replication monitor** page appears.
2. Select the tab for the replication type:
The **Periodic tab** shows information about replication that is performed on a scheduled basis.

For more information, see [Periodic Replication Monitoring](#)

Performing failover

Part of any valid Disaster Recovery (DR) plan is the test plan which is executed frequently to ensure the organization can recover in a true DR event.

See [Testing Failover](#) for the process of testing a 'failover'.

See [Scheduling Planned Failovers and Test Boots](#) for more advanced test scenarios.

Performing fallback

After testing or after the primary site has been returned to full working operation, you will need to perform a **Failback**.

Follow [Performing a Failback Operation](#) to fallback to the original processing site or region.

Monitoring Commvault with AWS CloudWatch

Commvault configures a number Amazon CloudWatch alarms to continually monitor and alarm conditions that require attention. In fact, CloudWatch is configured to automatically act for certain events.

Reboot Alarms

Commvault configures an alarm with name **Reboot Alarm for Commvault Backup and Recovery - <Stack name>**.

This alarm has the following characteristics:

- Monitors the [StatusCheckFailed_Instance](#) metric for instance status check response
 - Instance status checks monitor the software and network configuration of your individual instance. Amazon EC2 checks the health of the instance by sending an address resolution protocol (ARP) request to the network interface (NIC). These checks detect problems that require your involvement to repair. When an instance status check fails, you typically must address the problem yourself (for example, by rebooting the instance or by making instance configuration changes). ([source](#))
- If the instance status checks fail more than five (5) times, a reboot is triggered

Activity Alarms

Commvault configures an alarm with name **Recovery Alarm for Commvault Backup and Recovery - <Stack name>**. This alarm has the following characteristics:

- Monitors the [StatusCheckFailed_System](#) metric for system status check response

- System status checks monitor the AWS systems on which your instance runs. These checks detect underlying problems with your instance that require AWS involvement to repair. When a system status check fails, you can choose to wait for AWS to fix the issue, or you can resolve it yourself.

For instances backed by Amazon EBS, you can stop and start the instance yourself, which in most cases results in the instance being migrated to a new host. ([source](#))

- If the system status checks fail more than fifteen (15) minutes, a reboot is triggered

Diskspace Alarms and notifications

Commvault has several Amazon EBS volume(s) that function together to provide intelligent data management and protection across your cloud, SaaS, and edge-based workloads. Commvault configures an Amazon CloudWatch disk space alarm during deployment called **Disk Space Alarm for Commvault Backup and Recovery - <Stack name>**, the alarm has the following characteristics:

- Receives Amazon CloudWatch **LogicalDisk % Free Space** usage metrics periodically.
- If free space (%) drops below 30%, an alarm is generated.
- The alarm is sent to a Simple Notification Service (SNS) Topic, which then delivers an **email notification** to the administrator to investigate.

Using the License Summary Report to understand usage

When subscribing to the Commvault Backup & Recovery **AMI-used** product, there are three main licensing meter(s) to monitor. These are:

- **Per-VM** usage, which is consumed by Amazon EC2, EKS, EKS-D, Outposts EC2 & EKS, Red Hat OpenShift on AWS, and VMware Cloud on AWS protection, also tracks and consumes protection in other clouds and on-premises hypervisors and Kubernetes clusters.
- **Structured TB** usage which is consumed by Amazon Aurora, DocumentDB, DynamoDB, RDS, and Redshift databases. This license also tracks and consumes non-virtual and file protection for structured data on other clouds and on-premises physical hosts.
- **Unstructured TB** usage, which is consumed by Amazon EFS, FSx, Storage Gateway, and S3 protection. This license also tracks and consumes protection in other clouds and on-premises for non-virtual file and object data.

The best source of data on your usage is your [Billing Dashboard](#). But should you want to see which hosts, instances, or clusters are consuming Commvault Backup & Recovery licenses, you can use the [License Summary Report](#).

Reports / License summary

Details of purchased and used licenses.

Commcell

Usage as of: Sep 6, 2021, 12:00:02 AM License expiration: Sep 02, 2022 Recalculate More Info

Capacity Licenses

Commvault Complete OI Licenses

License	Available Total	Used	Summary
Operating Instances	0	5	License not purchased
Virtual Operating Instances	500	12	2.40%

1 - 2 of 2 items

Virtualization Licenses

License	Available Total	Used	Summary
VM Sockets	0	0	License not purchased
Protected Virtual Instances	0	11	License not purchased
Archived VMs	0	0	License not purchased
Application Class Virtual	0	0	License not purchased
DR VM	500	5	1.00%

1 - 5 of 5 items

User Licenses

Activate Licenses

Metallic Licenses

Other Licenses

Virtual Machine usage

The **Per-VM** licensing dimension may be observed within the License Summary Report in two (2) separate sub-reports.

The **Licensed capacity** and **Virtual Machine** used quantity is found in **Commvault Complete OI Licenses** section (see below)

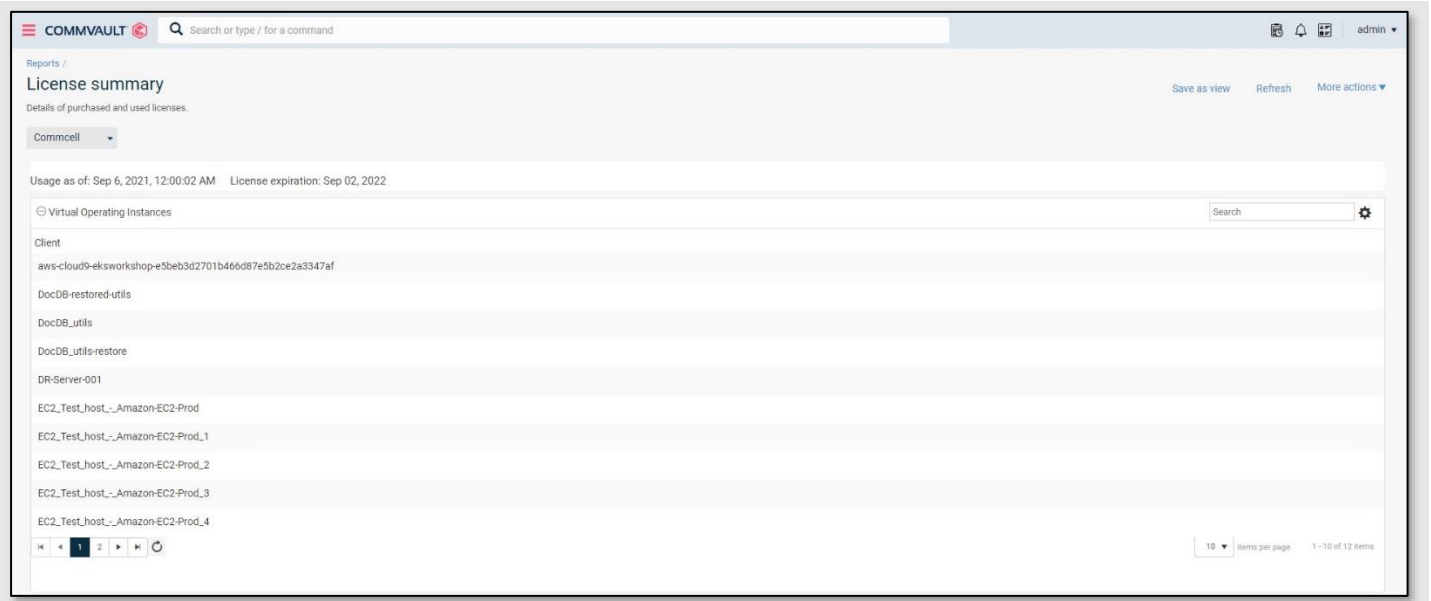
License	Available Total	Used	Summary
Operating Instances	0	5	License not purchased
Virtual Operating Instances	500	12	2.40%

1 - 2 of 2 items

The **Available Total** column indicates there are 500 clients licenses available on this system.

The **Used** column indicates there are **twelve (12)** protected instances.

Clicking the **Virtual Operating Instances** license name will open a drill-down report to show exactly which systems are consuming the licenses (see below).



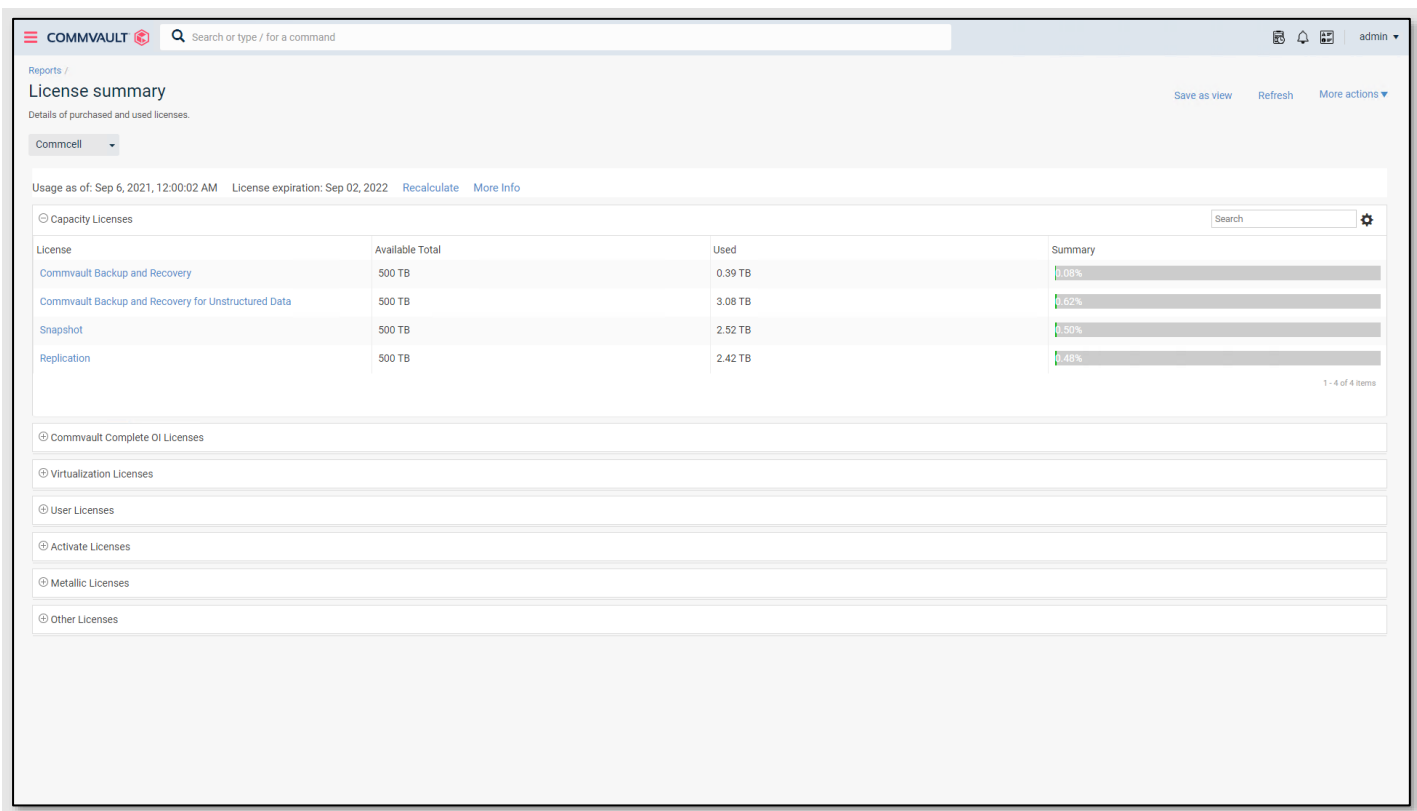
The drill-down report will include all **virtual instances** including Virtual Machines (Amazon EC2 instances) and Kubernetes Applications (Amazon EKS, EKS-D).

If a break-down between Virtual Machines and Kubernetes applications is required, the **Protected Virtual Instances** report shows the distinction between VM clients.

License	Available Total	Used	Summary
VM Sockets	0	0	License not purchased
Protected Virtual Instances	0	11	License not purchased
Archived VMs	0	0	License not purchased
Application Class Virtual	0	0	License not purchased
DR VM	500	5	1.00%

Structured TB usage

The **Per Structured TB** pricing/licensing dimension may be viewed within the **Capacity Licenses** section of the License Summary Report (see below)



Structured TB may be observed in one of three (3) drill-down reports:

- **Streaming backup** (Amazon RDS dump/export, Amazon DynamoDB) will be observed within the **Commvault Backup and Recovery** drill-down report.
- **Snapshot backup + replication** (Amazon RDS, DocumentDB, Redshift) will be observed within the **Snapshot** and **Replication** drill-down reports.

NOTE: Commvault will only meter usage for a single primary backup method (snapshot+replication or backup+archive).

Unstructured TB usage

The **Per Unstructured TB** pricing/licensing dimension may be viewed within the **Capacity Licenses** section of the License Summary Report (see below)

COMMVAULT Search or type / for a command admin

Reports / License summary Save as view Refresh More actions

Details of purchased and used licenses. Commcell

Usage as of: Sep 6, 2021, 12:00:02 AM License expiration: Sep 02, 2022 Recalculate More Info

Capacity Licenses Search

License	Available Total	Used	Summary
Commvault Backup and Recovery	500 TB	0.39 TB	0.08%
Commvault Backup and Recovery for Unstructured Data	500 TB	3.08 TB	0.62%
Snapshot	500 TB	2.52 TB	0.50%
Replication	500 TB	2.42 TB	0.48%

1 - 4 of 4 items

Commvault Complete OI Licenses

Virtualization Licenses

User Licenses

Activate Licenses

Metallic Licenses

Other Licenses

Unstructured TB may be observed within the **Commvault Backup and Recovery for Unstructured Data** drill-down report, which covers Amazon EFS, FSx, Storage Gateway, and S3 data.

Disaster Recovery usage

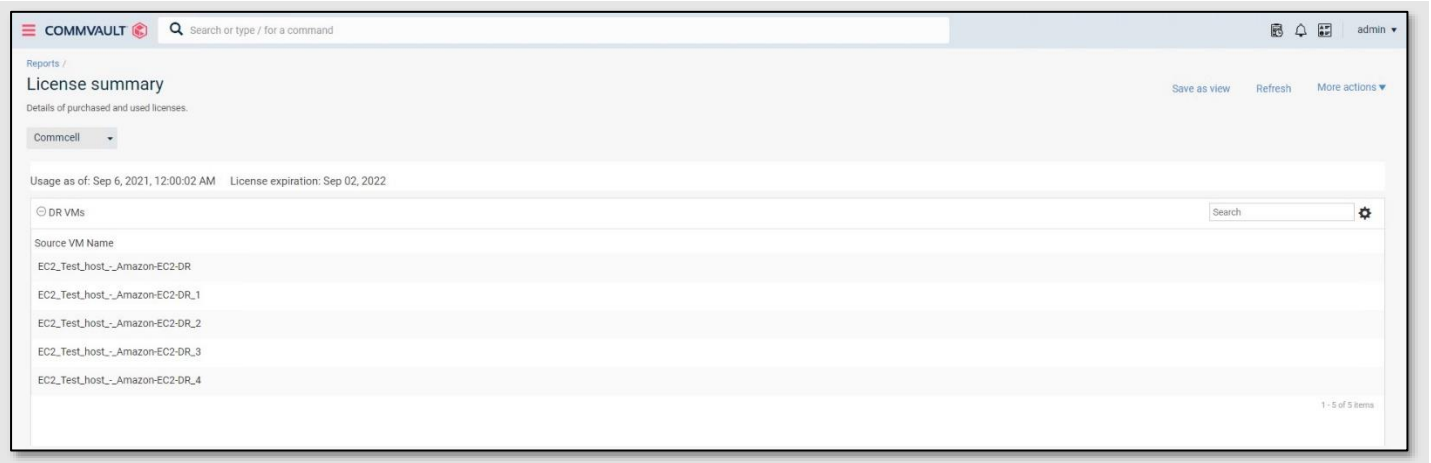
The **Per DR VM** licensing dimension may be observed within the License Summary Report within the **Virtualization Licenses** section of the License Summary Report. All DR VMs may be observed in the **DR VM** drill-down report.

Virtualization Licenses Search

License	Available Total	Used	Summary
VM Sockets	0	0	License not purchased
Protected Virtual Instances	0	11	License not purchased
Archived VMs	0	0	License not purchased
Application Class Virtual	0	0	License not purchased
DR VM	500	5	1.00%

NOTE: Retention for DR VM backups must be less than fourteen (14) days or the VM will incur a DR and a Backup license.

The drill-down report will identify each of the **source VMs** that are contributing to the DR VM consumption via an active replication relationship (see below).

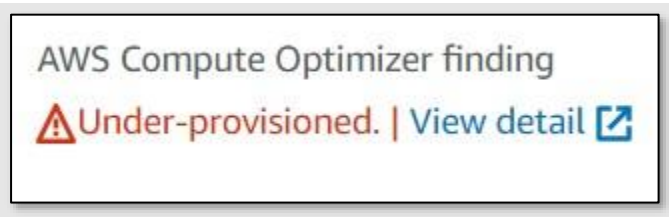


Optimizing Commvault in AWS Marketplace

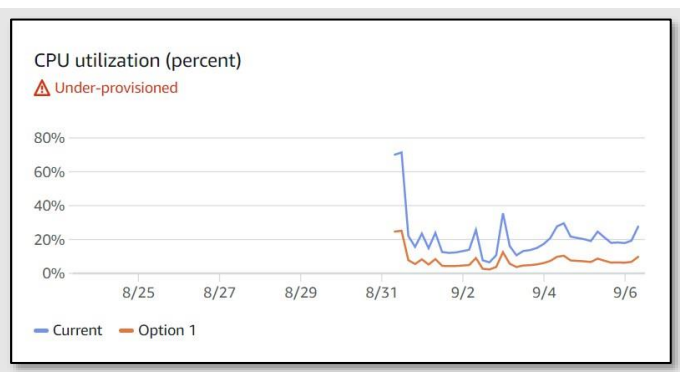
There are several tools available within the AWS cloud to assist in tuning the performance of your Commvault Backup & Recovery instance.

Using Amazon EC2 Optimizer to tune CPU and RAM

[AWS Compute Optimizer](#) can be used to observe CPU, RAM, and network resource consumption. Open your **Amazon EC2 Dashboard** and locate your Commvault Backup & Recovery instance. Under the **details** tab, there will be an observation from Compute Optimizer (see below)



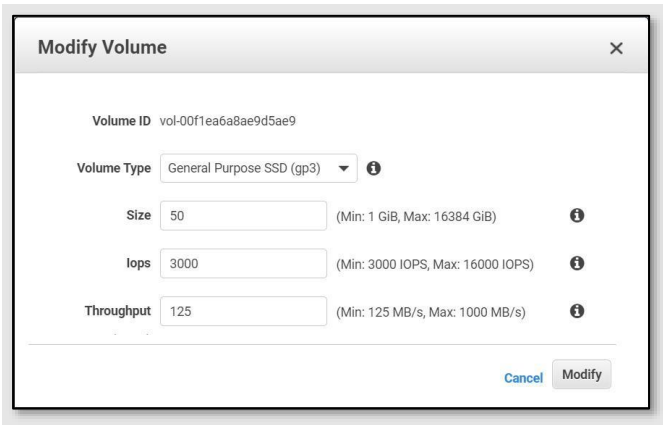
Click **View details** to see the findings, for example based on the current data available, Optimizer has assessed the current CPU allocation on this host as **Under provisioned**



Commvault recommends using Amazon EC2 Optimizer during planned maintenance activities to tune your instance resources up or down – based on observation. Be aware that tuning resources below the Commvault minimum requirements will result in sub-optimal backup and recovery performance.

Tuning Amazon EBS gp3 disk performance

[AWS Compute Optimizer](#) can now perform monitoring of IOPS and bandwidth consumption on EBS volumes. This information can be used to tune the IOPS and throughput on Commvault gp3 volumes. Simply right-click on the EBS volume, choose **Modify** and performance characteristics may be tuned (see below).



Modify Volume

Volume ID: vol-00f1ea6a8ae9d5ae9

Volume Type: General Purpose SSD (gp3)

Size: 50 (Min: 1 GiB, Max: 16384 GiB)

IOPS: 3000 (Min: 3000 IOPS, Max: 16000 IOPS)

Throughput: 125 (Min: 125 MB/s, Max: 1000 MB/s)

Cancel Modify

Terminating Commvault instances in AWS Marketplace

Commvault has placed several termination protections on data retention resources provisioned by the Commvault Backup & Recovery CloudFormation Template (CFT). This section details how to disable these protections and delete the protected resources after adequate analysis has occurred to ensure the resources are no longer required by the organization.

Disabling Amazon Instance EC2 Protection

To initiate a **Delete Stack** for your Commvault Backup & Recovery resources, you must first disable termination protection from your Commvault Backup & Recovery EC2 Instance. Perform the following steps to disable termination protection:

1. Login to the **AWS console**
2. Navigate to the **EC2 Dashboard** <https://console.aws.amazon.com/ec2/v2/home?region=us-east-1#Instances:>
3. Locate the instance you will be terminating, **right-click** > **Instance settings** > **Change termination protection**
4. Uncheck the **Enable** checkbox
5. Click **Save**

You can now proceed with deletion of the AWS CloudFormation Stack.

See [Enable Termination Protection](#) for more information on termination protection.

Manually deleting Amazon EBS volumes

After you successfully delete your AWS CloudFormation Stack, your Commvault Backup & Recovery EBS volumes will still exist within your account. This is intentional as the **DeleteOnTermination** attribute has been set to 'false' to ensure that deletion of Commvault data requires an additional administrative step.

See [Preserve Amazon EBS volumes on instance termination](#) for more information on the DeleteOnTermination protection.

To delete the volumes:

1. Login to the **AWS Console**
2. Navigate to the **EC2 Dashboard**

3. Click **Volumes**
4. Search by **tag:Created By** : and select the CloudFormation Stack to be deleted, all volumes are tagged to their original CloudFormation Stack, allowing easy identification of volumes.
5. Select all volumes
6. Choose **Actions ▼ / Delete Volumes**

Manually deleting Amazon S3 buckets

Commvault will not automatically delete the **Amazon S3 bucket** created during provisioning of your Commvault Backup & Recovery instance. To delete the bucket, after you have confirmed its contents are no longer required.

1. Login to **AWS Console**
2. Navigate to **S3 Dashboard**
3. Locate the **bucket**, select it.
4. Click **DELETE** button, you will need to enter the bucket name to delete.
NOTE: If the bucket contains data, you will need to click **EMPTY** first, and confirm deletion, then perform the DELETE

See [Emptying a bucket](#) and [Deleting a bucket](#) for more information.

Commvault and AWS CloudFormation

Commvault launches its industry leading Intelligent Data Services platform using the [AWS CloudFormation](#) infrastructure as code service. There are several CloudFormation Templates (CFTs) available for different purposes, they are described below.

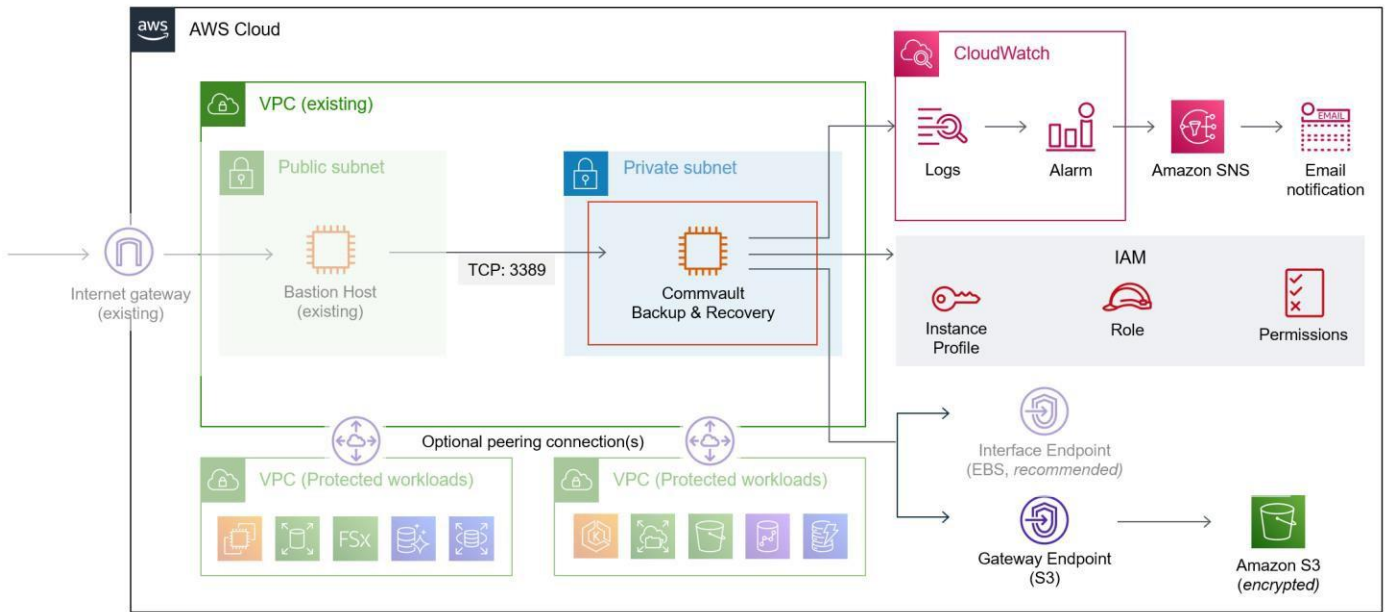
- **Commvault Backup & Recovery* – BYOL** is used to deploy bring your own license (BYOL) deployments of Commvault Backup & Recovery.
- **Standard deployment*** – is used when deploying the AMI-usage based Commvault Backup & Recovery product. This deployment provides a simplified day one launch experience with fixed subscription licensing quantities.
- **Custom deployment*** – is used when deploying the AMI-usage based Commvault Backup & Recovery product. This deployment provides a customized day one launch experience, allowing entry of customized subscription licensing quantities.
- **Additional deployment** – is used when expanding the number of Commvault Backup & Recovery environments within an existing VPC. This deployment provides a customized day one launch experience, allowing entry of customized subscription licensing quantities.

* These templates share common components (IAM role/policies, VPC IP, Subnet ID). Only one instance across these three deployment types is permitted within a single AWS account.

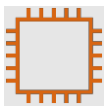




Multiple Commvault Backup & Recovery servers may be added after an initial deployment, using the **Additional deployment** template.

Components Deployed by AWS CloudFormation

Commvault consists of several integrated AWS services to deliver holistic, intelligent data management services across all AWS regions, AZs, and accounts. The following reference architecture shows the components deployed by the Commvault CloudFormation Templates (CFTs).



The following table details each of the components deployed.

Component Name	Purpose
 Commvault Backup & Recovery - <StackName> Amazon EC2 Instance	Amazon EC2 instance including Commvault Backup & Recovery software. Preconfigured on first boot.
 Commvault Backup & Recovery - <StackName> Amazon EC2 NetworkInterface	Amazon EC2 Elastic Network Interface (ENI) attached to Commvault Backup & Recovery EC2 instance. Secured by pre-configured security group (see below).
 Commvault Backup & Recovery - <StackName> Amazon EC2 EIP	<i>Not depicted above.</i> (Optional) Amazon EC2 Elastic IP (EIP) address attached to Commvault Backup & Recovery EC2 instance. Provides a static public IP address for accessing Commvault software.
 CommvaultBackupAndRecovery AWS IAM Role	<i>Not depicted above.</i> AWS Identity and Access Management (IAM) Role providing required policies and permissions to perform intelligent data management and protection. Also contains permissions to perform hourly metering to AWS Marketplace Metering service.
 Multiple AWS IAM Policy	Path: /Commvault/ AWS IAM Policies (managed, inline) for performing intelligent data management and protection, and AWS Marketplace metering. Attached to CommvaultBackupAndRecovery (above).

Sec group

CommvaultBackupAndRecovery

AWS IAM InstanceProfile

AWS IAM Instance Profile for

CommvaultBackupAndRecovery IAM Role that is attached to the Commvault Backup & Recovery - <Stackname> EC2 instance.

Path: /Commvault/

Commvault Backup & Recovery - <StackName>

AWS EC2 SecurityGroup

Amazon EC2 Security group and related

SecurityGroupIngress rules to secure incoming connections into the Commvault Backup & Recovery EC2 instance.

CvItS3Endpoint

AWS EC2 VPCEndpoint

(Optional) Amazon EC2 VPC Endpoint (Gateway type) for contacting Amazon S3 service from Commvault Backup & Recovery EC2 instance.

Recommended for cost reduction, performance, and security of data transferred to Amazon S3.

CvItRouteTable

AWS EC2 RouteTable

(Optional) Used to update relevant route table(s) within an existing VPC when a S3 VPC Endpoint is requested for creation.

Not depicted above.

Commvault Backup & Recovery - <StackName>

AWS S3 Bucket

An Amazon S3 Standard bucket with Server-Side Encryption (SSE-KMS) and Bucket keys enabled. Used to provide an initial Commvault Cloud Library for the Commvault Backup & Recovery EC2 instance.

Reboot Alarm for Commvault Backup and Recovery - <StackName>

AWS CloudWatch Alarm

Amazon CloudWatch alarm that triggers a reboot when an [instance status check](#) (StatusCheckFailed_Instance) fails for 5 consecutive minutes.

Recovery Alarm for Commvault Backup and Recovery - <StackName>

AWS CloudWatch Alarm

Amazon CloudWatch alarm that triggers a recovery when [instance status check](#) (StatusCheckFailed_System) fails for 15 consecutive minutes.

Disk Space Alarm for Commvault Backup and Recovery - <StackName>











AWS CloudWatch CompositeAlarm

Amazon CloudWatch alarm that takes logs from Amazon CloudWatch agent on Commvault Backup & Recovery instance, and triggers when disk space falls below 30% on any drive.

Commvault Backup and Recovery - <StackName>

AWS SNS Topic

Amazon Simple Notification Topic (SNS) Topic which receives notifications from the Disk Space Alarm (see above), and forwards to configured notification targets.

	<p>Commvault Backup and Recovery - <StackName></p> <p>AWS SNS Topic (Endpoint)</p>	<p>Amazon SNS subscription endpoint (email) with supplied administrator email. Forwards Disk Space Alarms to supplied administrator email address.</p>
		
		
		
		
		
		<hr data-bbox="756 1424 1015 1429"/>
		
		
		

There are several supporting LambdaFunctions for configuring networking, route tables, security groups, and applying consistent tagging across all elements. These have been omitted for brevity.

Use Encryption in AWS Marketplace Products

Commvault is committed to ensuring your data assets are secured in accordance with AWS and industry best practices. Use of **encryption** for stored and transmitted data is considered a 'must-have' in cloud and Commvault CloudFormation Templates (CFTs) deliver in this need.

Commvault leverages AWS encryption for all components deployed by Commvault, these being:

- **Amazon EBS encryption** is enabled for all created volumes with the default Amazon EBS encryption key for the region (aws/ebs). See Amazon [EBS encryption](#) for additional details.
- **Amazon S3 bucket encryption** is enabled on the created S3 bucket, intended for Commvault backup & archive data. Server-Side Encryption (SSE) is enabled using the aws:kms algorithm (see [Enabling Amazon S3 default bucket encryption](#) for more information). Additionally, S3 Bucket Keys are enabled to lower the cost of utilizing encryption with Amazon S3 (See Reducing [the cost of SSE-KMS with Amazon S3 Bucket Keys](#) for more information).

Customers are free to modify the CloudFormation template to select an alternate existing encryption key and/or alias.

Tagging in AWS Marketplace Products

Commvault applies several standard AWS tags to all created instances. See below for the tagging strategy applied to resources created by Commvault CloudFormation Templates (CFTs).

- All resources are tagged with **Name = Commvault Backup and Recovery - <StackName>**
- All resources are tagged with **Created By = Commvault Backup and Recovery - <StackName>**

Where <StackName> is the name of the AWS CloudFormation stack that created the resource.

Additionally, Commvault already uses tagging extensively within the product:

- Tag **_GX_BACKUP_** is applied to any resources created during a Commvault backup activity (Amazon EBS volumes, Amazon EBS, RDS, Redshift, DocumentDB snapshots and Amazon AMIs). When found on Amazon Machine Images (AMIs), it contains the value of the Amazon EC2 instance it protects.
- Tag **Name = CV_CBT_Snap** is applied to any resources created during a Commvault backup activity (Amazon EBS volumes, AMIs)
- Tag **Name = SP_N_XXX_YYY** is applied to any Amazon RDS, Redshift, and DocumentDB snapshots orchestrated by Commvault backup activity. These are for Commvault internal use.
- Tag **CV_Subclient** is set to the Commvault internal subclient or VM group that initiated the protection operation.
- Tag **CV_Retain_Snap** is applied to any Amazon service snapshots that are managed by Commvault IntelliSnap
- Tag **CV_Integrity_Snap** is applied to any Amazon service snapshots that are managed for the purposes of provide incremental forever protection, where a base integrity snapshot is maintained with one or more incremental dependent snapshots.
- Tag **Description = Snapshot_created_by_Commvault_for_job_NNN_at_XXXXXXXXXX._Source_Volume_vol-VOLID_from_INSTANCE-HOSTNAME** is set for EBS, RDS, Redshift and DocumentDB snapshots orchestrated by Commvault backup operations.
- Tag **CSIVolumeSnapshotName** is set on EBS snapshots (to the value of the CSI snapshot) when using [Kubernetes protection](#) with [Amazon EBS Container Storage Interface \(CSI\) driver](#).

Termination Protection

Protecting your data within and beyond cloud is crucial to recovering your business services when unplanned events strike. For this reason, Commvault has enabled multiple protections to prevent the accidental deletion or termination of critical Commvault Backup & Recovery data repositories. The protections include:

- **Amazon EC2 Termination Protection** is enabled by default on the Commvault Backup & Recovery instances (see [How do I protect my data against accidental EC2 instance termination?](#) for more information).
- **DeleteOnTermination** is disabled by default on all Commvault Backup & Recovery volumes to prevent accidental deletion of core Commvault backup data on termination (see [Preserve Amazon EBS volumes on instance termination](#) for more information)
- **DeletionPolicy** for the created Amazon S3 Bucket is set to 'Retain' to ensure that removal of your Amazon CloudWatch Stack will not accidentally delete all backup data written to the S3 bucket (See [DeletePolicy attribute](#) for more information).

AMI Drive Layout

Commvault has several software components that work together to provide intelligent data management services across all your data locations. Each volume has a different IOPS, throughput, and capacity requirements depending on your individual data protection needs. The following section details the multiple Amazon EBS volumes deployed with each product, and their intended use.

Commvault Backup & Recovery Drive Layout

Commvault Backup & Recovery is an all-in-one Commvault CommServe® server, the following EBS volumes are created during initial provisioning. Commvault has minimized the size of each volume, each volume may be independently increased online when required (See [Extend a Windows file system after resizing a volume](#) for more information).

NOTE: Commvault deploys an Amazon CloudWatch alarm to notify the administrator via email when a volume falls below 30% free space. This allows adequate time to review and increase the storage volume if required.

Volume Mount Path [Label]	Vol. type	IOPS	Throughput (MB/s)	Capacity (GiB)	File-sys Block size	Volume Usage
C:\ [WINOS]	gp3	3000	125	35	NTFS 4K	Microsoft Windows Server Operating System
E:\ [CVLT]	gp3	3000	125	60	NTFS 4K	Commvault binaries, log files, and software cache
F:\ [MSSQL]	gp3	3000	125	40	NTFS 65K	Commvault MS SQL database files
G:\ [TLOGS]	gp3	3000	125	10	NTFS 65K	Commvault MS SQL database transaction logs
H:\ [DDB1]	gp3	3000	125	50	NTFS 32K	Commvault Deduplication Database IOPS requirements for DDB
I:\ [INDEXC]	gp3	3000	125	50	NTFS	Commvault MediaAgent Index Cache

					32K	IOPS requirements for Index Cache
J:\ [JOBS]	gp3	3000	125	50	NTFS 4K	Commvault Job results , 3DFS cache , DR backups and temporary upgrade files

Commvault Access Node Drive Layout

Commvault Access Node(s) are an all-in-one Commvault MediaAgent + Access Node + Cloud Apps data mover host. Access Nodes may be used to perform cloud-native snapshot creation and replication, and streaming data from clients to Commvault cloud libraries.

The following are the default EBS volumes and paths deployed to support any/all data management and protection use-cases.

Volume Mount Path [Label]	Vol. type	IOPS	Throughput (MB/s)	Capacity (GiB)	File-sys Block size	Volume Usage
nvme1n1 vg_commvault	gp3	3000	125	80	n/a	LVM2 Volume group for Commvault binaries, log files, index cache, and jobresults.
lv1 /opt/commvault	gp3	3000	125	(10)	xfs default	Commvault binaries. Commvault software cache.
lv2 /var/opt/commvault	gp3	3000	125	(4.9)	xfs default	Commvault log files.
lv3 /mnt/commvault_jobresults	gp3	3000	125	(40)	xfs default	Commvault job results folder, 3DFS cache, and FBR cache directory.
lv4 /mnt/commvault_indexcache	gp3	3000	125	(25)	xfs default	Commvault MediaAgent index cache location.
nvme2n1 vg_commvault_2	gp3	3000	125	25	n/a	LVM2 Volume group for Commvault Deduplication Database (DDB).

lv_ddb /mnt/commvault_ddb	gp3	3000	125	(20)	xfv default	Commvault Deduplication DataBase (DDB).
------------------------------	---------------------	------	-----	------	----------------	---

BYOL Deployment

The 'BYOL Deployment' Amazon CloudFormation Template (CFT) deploys a single Amazon EC2 instance containing the latest Commvault Backup & Recovery software pre-installed and configured. The sections below detail each of the **parameters** requested during deployment and how to set them.

Specify Stack Name

- **Stack name**

Stack name can include letters (A-Z and a-z), numbers (0-9), and dashes (-).

*Stack name is appended to the **Name** and **Created By** tags to provide traceability of all components created by Commvault. Stack name being particularly important when deploying more than one Commvault instance in a single VPC or account.*

Stack name

Stack name

Stack name can include letters (A-Z and a-z), numbers (0-9), and dashes (-).

Step One - Select your EC2 Instance configuration

- **EC2 Instance Type**

Select instance size by the number of protected EC2 + EKS instances - [m5a/m5.xlarge - up to 100 instances] [m5a/m5.2xlarge - up to 500 instances] [t3a.2xlarge - dev/test].

Default is a m5a.2xlarge. Commvault recommends starting small and increasing instance size only when protected data volumes dictate an increase. See [Hardware Specifications for the CommServe Server](#))

- **EC2 Key Pair**

Select an existing EC2 Key Pair to access your Commvault Backup & Recovery Server.

Be sure you have access to the selected Key Pair. You will need this to obtain your login credentials to your Commvault Backup & Recovery instance (See - [How do I retrieve my Windows administrator password after launching an instance?](#)).

- **Administrator Email**

Enter the email address which will receive Amazon CloudWatch disk space alarms.

Required for Amazon CloudWatch disk space alarms to send email to the administrator if any Commvault Backup & Recovery instance disk volume reaches less than 30% free space. See – [How would a user](#)

[subscribe for notifications to be delivered over email?](#) for details on accepting the subscription activation request from no-reply@sns.amazonaws.com.

Parameters

Parameters are defined in your template and allow you to input custom values when you create or update a stack.

Step One - Select your EC2 Instance configuration

EC2 Instance Type

Select instance size by the number of protected EC2 + EKS instances - [m5a/m5.xlarge - up to 100 instances] [m5a/m5.2xlarge - up to 500 instances] [t3a.2xlarge - dev/test].

m5a.2xlarge

EC2 Key Pair

Select an existing EC2 Key Pair to access your Commvault Backup & Recovery Server.

Administrator Email

Enter the email address which will receive Amazon CloudWatch disk space alarms.

Step Two - Select your network configuration

- **VPC ID**

Select an existing VPC.

You must select an existing [Amazon Virtual Private Cloud \(VPC\)](#) visible to the AWS account. The VPC may be local to authenticated AWS account or may be peered from another region or another account (see [What is VPC peering?](#) for more information).

NOTE: If you would like to isolate Commvault to a dedicated VPC, please pre-create the VPC and associated Subnets prior to launching CloudFormation.

- **Subnet ID**

Select an existing Subnet.

You must select an existing [Amazon VPC Subnet](#) visible to the AWS account. The Subnet may be local to authenticated AWS account or may be peered from another region or another account (see [What is VPC peering?](#) for more information).

- **Elastic IP**

Select [true] to provision an Elastic IP (EIP) for Commvault Backup & Recovery Server.

Default: **false**

Set to **true** if you would like a static public IP address or [Elastic IP Address](#) provisioned for Commvault.

Set to **false** if you will be using private addressing only for Commvault, and accessing via a bastion host.

See [Controlling Network Access to EC2 Instances Using a Bastion Server](#) for more information.

- **Authorized Admin Subnet**

Enter a comma-delimited list of CIDR blocks (Subnets, Hosts) that will access Commvault via RDP (for example, 10.0.0.1/24, 199.147.238.4/32) Note: 0.0.0.0/0 is not supported

Enter a single host or a CIDR block where your trusted administrative hosts reside.

A virtual firewall or [security group](#) will be provisioned allowing incoming Remote Desktop Protocol (RDP) from the supplied Authorized Subnet.

- **Protected Subnets**

Select the subnets that contain data to protect.

Commvault software agents may be installed into remote VPCs and Subnets. Ongoing data management and protection operations will require communication between the Commvault Backup & Recovery instance and Amazon EC2 infrastructure running Commvault software agents. Select subnets you would like to authorize for incoming connections to the Commvault Backup & Recovery instance on ports 443, 8400, and 8403. (see [Port Requirements for Commvault](#) for details of how each port is used)

NOTE: If your network security only permits outgoing connections from Commvault to protected hosts, simply select the CommServe subnet only.

- **S3 VPC Endpoint**

Do you have an existing Amazon S3 VPC Endpoint available in your VPC ?

Default: **true**


*Set to **false** if you do not have an Amazon S3 VPC Endpoint defined in the target VPC. Commvault will create a new S3 VPC Endpoint (Gateway type).*

*Set to **true** (default) if you already have an existing Amazon S3 VPC Endpoint within the target region.*

Acknowledge IAM Role Creation

Commvault will be creating an IAM Role with required permissions for Amazon service data management and protection. Acknowledge the permission to create IAM Roles when prompted (see below)

ⓘ The following resource(s) require capabilities: [AWS::IAM::Role]

This template contains Identity and Access Management (IAM) resources. Check that you want to create each of these resources and that they have the minimum required permissions. In addition, they have custom names. Check that the custom names are unique within your AWS account. [Learn more](#) 

I acknowledge that AWS CloudFormation might create IAM resources with custom names.

Commvault Backup & Recovery: Standard Deployment

The **Standard Deployment** method is used when deploying an initial Commvault Backup & Recovery instance to an account and/or VPC.

The BYOL, Standard, and Custom deployment templates share the same Identity & Access Management (IAM) Role definitions – so only one instance may be deployed within an account, across all three templates.

Common steps

Standard deployment shares the following settings with the BYOL template:

- [Specify Stack Name](#)
- [Step One - Select your EC2 Instance configuration](#)
- [Step Two - Select your network configuration](#)

There is an additional step before Stack creation.

Step Three - Select your initial starter pack (annual subscription, upfront payment)

This step configures your initial software subscription amounts. Your Commvault Backup & Recovery subscription includes two (2) primary usage types:

- **Starter packs** which are annual subscriptions, paid upfront as part of your next AWS monthly invoice.
- **Overage** usage which is any consumption above the starter pack volume(s), charged daily, invoiced monthly.

Step Three - Select your initial starter pack (annual subscription, upfront payment)

Backup and Recovery For Virtual Machines
Virtual instances (EC2 instances, EKS applications) are licensed in bundles of 10, please enter the number of 10-packs required (min. 5, max. 9999).

Backup and Recovery For Structured Data
Select the total size in Terabytes (TB) for protected Aurora, RDS, DynamoDB, DocumentDB, and Redshift instances.

Backup and Recovery For Unstructured Data
Select the total size in Terabytes (TB) for protected S3, EFS, FSx, and Storage Gateway instances.

Complete the **initial Starter Pack** section by selecting an initial subscription volume for each data type:

- **Backup and Recovery for Virtual Machines**
Virtual instances (EC2 instances, EKS applications) are licensed in bundles of 10, please select the number of 10-packs required (min. 5, max. 50).

Protection of Amazon EC2, VMware Cloud on AWS, and EKS instances is metered to this license. Additionally, protection of on-premises and other-cloud VMs and Kubernetes applications is metered to this license. Select from pre-defined volumes of 5, 10, 25, and 50 VM10 packs.

NOTE: Each unit protects ten (10) Virtual Instances (for example, 5 represents 5 x 10 or 50 individual VMs).

- **Backup and Recovery for Structured Data**
Select the total size in Terabytes (TB) for protected Aurora, RDS, DocumentDB, DynamoDB, and Redshift instances.

Select from pre-defined volumes of 50, 100, 250, and 500 Terabytes (TB) for snapshot and streaming protection of Amazon Aurora, DocumentDB, RDS, and Redshift data.

- **Backup and Recovery for Unstructured Data**
Select the total size in Terabytes (TB) for protected S3, EFS, FSx, and Storage Gateway instances.

Select from pre-defined volumes of 50, 100, 250, and 500 terabytes (TB) for streaming protection of Amazon EFS, FSx, S3, and Storage Gateway (File Gateway) data.

You may now continue onto [Acknowledge IAM Role Creation](#) before final stack creation.

Commvault Backup & Recovery: Custom Deployment

The **Custom Deployment** method is used when deploying an initial Commvault Backup & Recovery instance to an account and/or VPC.

The BYOL, Standard, and Custom deployment templates share the same Identity & Access Management (IAM) Role definitions – so only one instance may be deployed within an account, across all three templates.

Common steps

Additional deployment shares the following settings with the BYOL template:

- [Specify Stack Name](#)
- [Step One - Select your EC2 Instance configuration](#)
- [Step Two - Select your network configuration](#)

There is an additional step before Stack creation.

Step Three - Select your initial starter pack (annual subscription, upfront payment)

This step configures your initial software subscription amounts. Your Commvault Backup & Recovery subscription includes two (2) primary usage types:

- **Starter packs** which are annual subscriptions, paid upfront as part of your next AWS monthly invoice.
- **Overage** usage which is any consumption above the starter pack volume(s), charged daily, invoiced monthly.

Step Three - Select your initial starter pack (annual subscription, upfront payment)

Backup and Recovery For Virtual Machines
Virtual instances (EC2 instances, EKS applications) are licensed in bundles of 10, please enter the number of 10-packs required (min. 5, max. 9999).

Backup and Recovery For Structured Data
Enter the total size in Terabytes (TB) for protected Aurora, RDS, DynamoDB, DocumentDB, and Redshift instances (min. 50, max. 9999).

Backup and Recovery For Unstructured Data
Enter the total size in Terabytes (TB) for protected S3, EFS, FSx, and Storage Gateway instances (min. 50, max. 9999).

Custom deployment differs from a Standard deployment by allowing the user to enter preferred subscription license quantities vs. selecting from pre-set quantities.

Complete the **initial Starter Pack** section by selecting an initial subscription volume for each data type:

- **Backup and Recovery for Virtual Machines**
Virtual instances (EC2 instances, EKS applications) are licensed in bundles of 10, please enter the number of

10-packs required (min. 5, max. 9999).

Protection of Amazon EC2, VMware Cloud on AWS, and EKS instances is metered to this license. Additionally, protection of on-premises and other-cloud VMs and Kubernetes applications is metered to this license. Enter a value between 5 and 9999.

NOTE: Each unit protects ten (10) Virtual Instances (for example, 5 represents 5 x 10 or 50 individual VMs).

- **Backup and Recovery for Structured Data**

Select the total size in Terabytes (TB) for protected Aurora, RDS, DocumentDB, DynamoDB, and Redshift instances.

Enter a number between 50 and 9999 for the total subscribed Structured terabytes (TB) for snapshot and streaming protection of Amazon Aurora, DocumentDB, RDS, and Redshift data.

- **Backup and Recovery for Unstructured Data**

Select the total size in Terabytes (TB) for protected S3, EFS, FSx, and Storage Gateway instances.

Enter a number between 50 and 9999 for the total subscribed Unstructured terabytes (TB) for streaming protection of Amazon EFS, FSx, S3, and Storage Gateway (File Gateway) data.

You may now continue onto [Acknowledge IAM Role Creation](#) before final stack creation.

Commvault Backup & Recovery: Additional Deployment

Common steps

Additional deployment shares the following settings with the BYOL template:

- [Specify Stack Name](#)
- [Step One - Select your EC2 Instance configuration](#)

There are some additional steps before Stack creation.

Step Two - Select your network configuration

- **Subnet ID**
Select an existing Subnet.

You must select an existing [Amazon VPC Subnet](#) visible to the AWS account. The Subnet may be local to authenticated AWS account or may be peered from another region or another account (see [What is VPC peering?](#) for more information).

- **Existing Security Group ID**
Select an existing Security Group.

Select an existing Security Group previously created by deployment of the BYOL, Standard, or Custom deployment CloudFormation templates. Alternatively, you can manually clone the existing Commvault Backup

& Recovery Security group for this new instance and select new group here.

- **Elastic IP**

Select [true] to provision an Elastic IP (EIP) for Commvault Backup & Recovery Server.

Default: **false**

Set to **true** if you would like a static public IP address or [Elastic IP Address](#) provisioned for Commvault.

Set to **false** if you will be using private addressing only for Commvault, and accessing via a bastion host.

See [Controlling Network Access to EC2 Instances Using a Bastion Server](#) for more information.

Step Three - Select your initial starter pack (annual subscription, upfront payment)

This step configures your initial software subscription amounts. Your Commvault Backup & Recovery subscription includes two (2) primary usage types:

- **Starter packs** which are annual subscriptions, paid upfront as part of your next AWS monthly invoice.
- **Overage** usage which is any consumption above the starter pack volume(s), charged daily, invoiced monthly.

Step Three - Select your initial starter pack (annual subscription, upfront payment)

Backup and Recovery For Virtual Machines
Virtual instances (EC2 instances, EKS applications) are licensed in bundles of 10, please enter the number of 10-packs required (min. 5, max. 9999).

Backup and Recovery For Structured Data
Enter the total size in Terabytes (TB) for protected Aurora, RDS, DynamoDB, DocumentDB, and Redshift instances (min. 50, max. 9999).

Backup and Recovery For Unstructured Data
Enter the total size in Terabytes (TB) for protected S3, EFS, FSx, and Storage Gateway instances (min. 50, max. 9999).

Additional deployment differs from a Standard deployment by allowing the user to enter preferred subscription license quantities vs. selecting from pre-set quantities.

Complete the **initial Starter Pack** section by selecting an initial subscription volume for each data type:

- **Backup and Recovery for Virtual Machines**

Virtual instances (EC2 instances, EKS applications) are licensed in bundles of 10, please enter the number of 10-packs required (min. 5, max. 9999).

Protection of Amazon EC2, VMware Cloud on AWS, and EKS instances is metered to this license.

Additionally, protection of on-premises and other-cloud VMs and Kubernetes applications is metered to this license. Enter a value between 5 and 9999.

NOTE: *Each unit protects ten (10) Virtual Instances (for example, 5 represents 5 x 10 or 50 individual VMs).*

- **Backup and Recovery for Structured Data**

Select the total size in Terabytes (TB) for protected Aurora, RDS, DocumentDB, DynamoDB, and Redshift instances.

Enter a number between 50 and 9999 for the total subscribed Structured terabytes (TB) for snapshot and streaming protection of Amazon Aurora, DocumentDB, RDS, and Redshift data.

- **Backup and Recovery for Unstructured Data**

Select the total size in Terabytes (TB) for protected S3, EFS, FSx, and Storage Gateway instances.

Enter a number between 50 and 9999 for the total subscribed Unstructured terabytes (TB) for streaming protection of Amazon EFS, FSx, S3, and Storage Gateway (File Gateway) data.

You may now continue onto [Acknowledge IAM Role Creation](#) before final stack creation.

Related information

- [AWS CloudFormation](#)
- [AWS CloudFormation - documentation](#)