Commvault Platform Release 2024 Newsletter

Version: 11.34

December 15, 2023

Contents

Complete Backup And Recovery

Faster Backups and Browse Operations with Offline Cataloging for File System Block-Level Backups

For faster file system backup and browse operations, you can catalog files offline as a separate job after the block-level backup completes.

Key Features

- Faster backups: The cataloging job runs as a separate job which results in faster backups.
- Quick browse: Files are cataloged for efficient browse performance.

More Information

- Enabling Block-Level Backups for File System Agent

Log and Load Copy Backups for DB2 and DB2 MultiNode Databases Using Disk Caching for Frequent Log Backups

You can perform log and load copy backups for DB2 and DB2 MultiNode database clients through disk caching for frequent log backups.

Applicable Agents

- DB2
- DB2 MultiNode

More Information

- Adding an Automatic Database Log Backup Schedule to a Schedule Policy
- Configurations for RPO

Introducing 1-Touch Recovery and Redesigned Virtualize Me in Command Center

You can now perform the 1-Touch recovery operation to restore your Windows and UNIX client computers from the Command Center. Also, the Virtualize Me operation to convert or restore a physical computer to virtual machine is simplified and has a new wizard which makes it easy for you to quickly restore your client environment from disasters.

Key Features

- Virtualize Me
- 1-Touch Recovery

Applicable Agents

- Windows
- UNIX

More Information

- Virtualize Me for Windows and UNIX Computers
- 1-Touch Recovery for Windows and Unix File Systems

Back Up and Restore Personal and Channel Chats for Teams Users

You can configure backups for Teams personal chats and channel chats. When you enable this feature, chats are backed up per unique user account. All posts in personal messages, posts in channel (team) chats, posts in multiple-user conversations, and posts in meeting chats are included in the backup content.

More Information

- Configuring Personal Chat and Channel Chat Backups

EWS Support for Archive and Journal Mailboxes

You can use Exchange Web Services (EWS) to create an email journaling app in on-premises environments and an email archiving app in both on-premises and hybrid environments. EWS replaces Microsoft's deprecated MAPI technology and allows you to continue to use email journaling and email archiving with Exchange 2013 and later versions.

More Information

- Creating an Email Journaling App for the Journal Mailbox
- Creating an Email Archiving App for the User Mailbox in an On-Premises Environment
- Creating an Email Archiving App for the User Mailbox in an Hybrid Environment

Performance Enhancements to Postgres Dump-Based Backups

Commvault support for protecting a DumpBasedBackupSet in PostgreSQL database includes the following enhancements:

- Support for PostgreSQL15.x
- Perform backup and restore operations using parallel Postgres jobs
- Support for including global objects in backups

More Information

- System Requirements (Command Center)
- Restoring One or More PostgreSQL Databases (Command Center)
- Enabling Backups for Global Objects in PostgreSQL Databases (Command Center)
- Using Parallel Jobs to Dump the PostgreSQL Database (Command Center)
- System Requirements (CommCell Console)
- Performing Restores from DumpBased Backup Set (CommCell Console)
- Enabling Backups for Global Objects in PostgreSQL Databases (CommCell Console)
- Using Parallel Jobs to Dump the PostgreSQL Database (CommCell Console)

"Backup Destinations" Tab for Plans

You can view and modify backup destinations on the "Backup Destinations" tab for a plan. On the tab, you can perform operations such as adding a region to a backup destination, adding a copy to a region, modifying a copy associated with a region, and running a backup copy for a snapshot copy.

More Information

- Modifying a Server Plan

New Dashboard View for Disk and Cloud Storage

The Command Center now includes an overview dashboard for both disk and cloud storage, that provide graphical information about the data written on the storage. The disk storage dashboard includes views for total and available capacity, data retention based on days, and the disk usage by plan and workload. The cloud dashboard displays the cloud vendor type and the data usage on the cloud. Trending for data growth and performance throughput are also provided for storage planning and tuning.

More Information

- Viewing the Dashboard for Disk Storage
- Viewing the Dashboard for Cloud Storage

Integration of Data Domain Boost Storage Library

The Commvault Data Domain Boost Storage Library is an integration between the Commvault data protection software and the Dell EMC Data Domain and PowerProtect DD deduplication storage systems. Commvault is a Dell DD Boost ecosystem partner and has incorporated the DD Boost SDK into the Commvault platform, which allows advanced levels of integration and feature support with no additional software or plug-ins. This integration gives you more control over data operations, for enhanced resiliency and more efficient data transfer during backups and restores.

Commvault provides the following integrations:

Data Domain Boost Access Library: This library provides a direct connection to the device through the SDK and writes data in the native Commvault format. You can take advantage of the integration without worrying about data expansion on the storage due to data format changes.

Data Domain Boost Client Library: This library enables MediaAgents and servers running workloads to be full featured clients of the Dell EMC Data Domain, leveraging the native APIs and client-side deduplication of the DD Boost SDK, with direct data movement to and from the storage device. This library is intended for new deployments of Data Domain Boost Storage Libraries because the data is written in a new format that is optimized for this use case.

More Information

- Data Domain Boost Storage Library

Enhanced Dashboard to Monitor HyperScale X Cluster

The HyperScale dashboard in the Command Center is enhanced to provide a comprehensive view of the status of the software, security configurations, key hardware components, and cluster health.

Using the dashboard view, you can quickly determine the systems or nodes that need immediate attention and drill down to view detailed reports for the nodes in the cluster. You can further customize the report to filter the view by storage pool, node, and status to easily monitor the problem area.

More Information

- HyperScale Dashboard

Virtual Image with Windows CommServe Server to Support CIS Level 1 Security Controls

The CIS Level 1 Hardened CommServe server virtual image is a Windows-based deployable virtual machine installed with the CommServe server software. The operating system, SQL Server instance, and IIS configuration is pre-hardened using CIS Level 1 benchmarks.

More Information

- Certifications and Compliance

Enhancements for MongoDB Big Data Protection

Commvault protects big data file systems and applications using the MongoDB Big Data agent. Restoring data has become simplified with the following enhancements:
Encrypted Databases:

- You can protect and restore MongoDB replica set clusters that have encrypted databases using a local key file mechanism.

Restore an entire MongoDB cluster to its current location (In place):

- Automatically configure authentication, TLS/SSL, mongos, and mongod settings based on the source cluster configuration.

Restoring a MongoDB Cluster to a Different Cluster (Out of Place):

- Automatically configure authentication, TLS/SSL, mongos, and mongod settings based on the destination cluster configuration.
- After performing a Discover operation on the destination cluster, the restore clients, data paths, and ports will be automatically selected during the out of place restore.

Applicable Agents

- MongoDB

More Information

- System Requirements for MongoDB
- Restoring a MongoDB Cluster to Its Current Location (In Place)
- Restoring a MongoDB Cluster to a Different Cluster (Out of Place)

Security IQ Dashboard

Security IQ dashboard provides organizations with a simplified approach to validate and improve Commvault security posture using data insights that drive actions, reduce cyber risks, and protect backups for clean data recoveries.

Key Features

Security IQ offers the following features:

- Security posture score to help identify new security recommendations.
- Over 23 security control recommendations including multi-person authorization controls.
- Quick view of backup and infrastructure anomaly conditions.
- Quick view of File Anomaly conditions.
- Latest Audit trail events.

More Information

- Security IQ Dashboard

Modern Authentication Support for Microsoft Office 365 Email Server

You can now configure modern authentication for Microsoft Office 365 email servers.

More Information

- Configuring an Email Server

Commvault support of CockroachDB iDA

You can back up the entire CockroachDB cluster and perform a restore and recovery to the same or a different database cluster.

More Information

- CockRoachDB

Back Up and Restore YugabyteDB Cluster Namespaces

You can back up YugabyteDB cluster namespaces (YSQL, YCQL), and perform a granular restore and recovery to the same or a different cluster.

Applicable Agents

YugabyteDB

More Information

- YugabyteDB

Support for Citrix Hypervisor (XenServer) and Huawei FusionCompute

Using Command Center, you can protect virtual machines that are hosted in Citrix Hypervisor (XenServer) and Huawei FusionCompute.

Key Features

- Back up VMs.
- Restore guest files and folders or full VMs.

More Information

- Citrix Hypervisor (XenServer)
- Huawei FusionCompute

Detect Malware with ThreatScan Predict

ThreatScan Predict leverages AI to scan for unknown and new zero-day threats with greater fidelity. Finding threats earlier in an attack can help limit the exposure for your organization and reduce the costs to cleanly recover, customers can fight bad AI with good AI capabilities.

More Information

- Threat Analysis

Complete: Manage New Workloads

Backup and Restore Apache Hive Databases and Tables

You can configure full and incremental backups up of Apache Hive databases and tables (both

managed and external) in the Hadoop cluster.

Databases and tables can be restored in-place, or can be renamed and restored to the same cluster or a different cluster.

Key Features

- Backups leverage source-side deduplication, compression, and encryption, to minimize the data transfer.
- Both backup and restore operations use multiple nodes, each performing parallel data transfer, maximizing throughput to meet recovery point objectives (RPOs) and recovery time objectives (RTOs).

Applicable Agents

Hadoop

More Information

- Apache Hive

Commvault Supports Kubernetes Clusters and Access Nodes Running on the Linux ARM64 Platform

Commvault's protection for Kubernetes workloads now supports Kubernetes clusters and access nodes running on the Linux ARM64 platform.

More Information

- System Requirements for Kubernetes

Configure Kubernetes Settings at the Application Group and Cluster Levels

Instead of the access node, you can now set up Kubernetes settings at the application group and cluster levels.

- Application group level:
  - Modify the resource limits for the Commvault temporary pods.
  - Convert backups to live volume backups when a Volumesnapshots snapshot fails or when a Volumesnapshots snapshot fails to change to readyToUse:True state.
- Cluster level:

- Specify a different image registry (such as for an air-gapped cluster) for Commvault temporary pods.
- Configure a namespace where Commvault CRDs and resource modifiers can be created.
- Increase the time for Commvault temporary pods to wait for Kubernetes activities.

Applicable Agents

- Kubernetes

More Information

- Application group level:
- Modify the Resource Limits for Commvault Temporary Pods
- Converting Backups to Live Volume Backups When a Volumesnapshots Snapshot Fails or When a Volumesnapshots Snapshot Fails to Change to readyToUse:True State
- Cluster level:
- Specify a Different Image Registry (Such as for an Air-Gapped Cluster)
- Configuring a Namespace for Commvault Resources
- Increasing the Time That Commvault Temporary Pods Wait for Kubernetes Activities

Complete: Protect Virtual Environments

Application-Aware Backups for VMWare Cloud Director VMs

You can perform application-aware backups for VMs that run under VMware Cloud Director and that host the following applications:

- Active Directory
- Microsoft Exchange
- Microsoft SharePoint
- Microsoft SQL Server
- MySQL
- Oracle database for Windows

This capability is supported only for streaming backups.

Applicable Agents

- Virtual Server Agent (VSA)
- VMware vCloud Director

More Information

- Application-Aware Backups
- Hypervisor Support and Requirements for Application-Aware Backups

- Application Support for Hypervisors

Application-Based Backups for the Virtual Server Agent

With application-based backups for virtualized workloads, you can perform application discovery for VMs selected within the VM group and configure backups by installing an in-guest application agent. You can create the VSA VM group schedules separate from the subclient backup schedules because VM groups and subclients are independent of each other. The application-based backup includes the following parts:

- Virtual Server Agent (VSA) backup: The VSA backup of the virtual machine can be a streaming backup or IntelliSnap backup.
- Application backup: The application backup is always a streaming backup, even when the VSA subclient is an IntelliSnap backup.

Key Features

You can restore application-based backup data for the following:

- Active Directory
- Microsoft SQL Server
- MySQL Agent
- Oracle

Applicable Agents

- Virtual Server Agent (VSA) for VMware

More Information

- Application-Based Backups for the Virtual Server Agent

Oracle Cloud Infrastructure for Private Cloud Appliance (PCA)

Commvault protects instances that are hosted in Oracle Cloud Infrastructure Private Cloud Appliance (PCA). You can configure an OCI hypervisor to represent an OCI Private Cloud Appliance (PCA).

Key Features

- Back up instances.
- Restore guest files and folders and full instances.
- Replicate instances for disaster recovery, with orchestration for failovers and failbacks.

More Information

- Oracle Cloud Infrastructure for Private Cloud Appliance (PCA)

Perform Attach Disk Restore and Disk Filtering During Backup for VMware Cloud Director

With VMware Cloud Director, you can now filter the VM disks during a backup operation at the VM group level and perform an attach disk restore of VM disks.

More Information

- Managing VM Group Content for VMware Cloud Director
- Attaching a Disk to an Existing VM for VMware Cloud Director

Back Up and Recover Amazon DynamoDB Standard-Infrequent Access Instances

You can now protect Amazon DynamoDB instances configured with the Standard-Infrequent Access (DynamoDB Standard-IA) table class. This table class is ideal for use cases that require long-term storage of data that is infrequently accessed, such as application logs. You can now use Commvault to protect and restore DynamoDB workloads that use the Standard-IA table class.

Before this release, Commvault supported the protection of the Amazon DynamoDB Standard table class. This meant that DynamoDB instances with large amounts of long-term retention but infrequently accessed data such as application logs, social media posts, e-commerce order history, and gaming achievements could not leverage the storage cost savings of the DynamoDB Standard-Infrequent Access table class.

With this release, Commvault protects DynamoDB workloads that utilize DynamoDB Standard and DynamoDB Standard-Infrequent Access table classes. Commvault supports full and incremental backups of DynamoDB tables across accounts and AWS Regions. Individual tables, multiple tables, or all DynamoDB tables may be restored within and across AWS Regions and accounts.

Key Features

- Full and incremental backup support for DynamoDB Standard-Infrequent Access and DynamoDB Standard table classes
- Support for DynamoDB tables that change table class between Standard and Standard-Infrequent Access
- Recovery in-place, or to different AWS Regions or accounts with optional rename functionality

Setup Requirements

- Linux or Windows access node with the Virtual Server package installed
- Support for IAM role, access and secret key, and STS assume role with IAM policy authentication

More Information

- Amazon DynamoDB

Power Management for a MediaAgent Deployed on Oracle Cloud Infrastructure

You can use power management for a MediaAgent deployed on Oracle Cloud Infrastructure (OCI).

More Information

- Cloud MediaAgent Power Management

Credential Manager for Nutanix AHV Clients

You can use Commvault's Credential Manager to save and edit Nutanix AHV hypervisor credential entities. These credentials can be re-used with multiple Nutanix hypervisors.

Applicable Agents

Virtual Server Agent for Nutanix AHV Platform

More Information

- Configuring Backups for Nutanix AHV

Disaster Recovery

Test Failover for Google Cloud Platform

You can perform test failovers of VMs that are hosted on Google Cloud Platform (GCP) to test and optimize recovery readiness.

Use test failovers to recover test VMs to a network of your choice. After the test VMs are up and running

in the network, you can perform recovery fire drills to practice and optimize recovery processes. This approach to recovery planning empowers you to respond to unforeseen events and maintain the resilience of your GCP infrastructure.

More Information

- Failover Groups

Enhancements to Continuous Replication Using VAIO for VMware

Continuous replication using VAIO for VMware in Commvault includes the following enhancements:

- You can use Linux machines as access nodes.
- You can share the RP store with access nodes from the Command Center.

More Information

- System Requirements for Continuous Replication
- Sharing RP Store with Access Nodes

Use Scripts to Customize Pre and Post Failover and Failback Operations

In recovery groups and failover groups, you can use custom scripts to execute functions that must run pre-failover, post-failover, pre-failback, and post-failback. You can configure these settings for an entire recovery group or for individual VMs in a recovery group.

More Information

- Adding Customization Scripts for a Replication Group
- Adding Customization Scripts for Individual VMs in a Replication Group
- Adding a Pre Script for a Failover Group
- Adding a Post Script for a Failover Group

Undo Failover for Amazon EC2 Instances

Undo failover support for Amazon EC2 instances reduce the time required to switch from DR to the primary site and enables you to discard changes on the DR VM.

With undo failovers, you can do the following:

- Conduct audits, validations, and DR drills in the DR site.
- Simulate DR scenarios to validate recovery readiness and to recover SLAs.
- Discard changes in the DR site when the recovered data is corrupted.

During a failover operation, you can enable or disable the failover capability. After a failover, integrity snapshots are retained.

Note: The **Deploy Virtual Machine during failover** option has been deprecated. Now, by default, your virtual machines in the DR site are deployed only during failover for optimizing DR site costs and preventing accidental changes to DR virtual machines.

More Information

- Cross-Platform Feature Support for Auto-Recovery
- Failover Groups
- Undoing a Failover

Virtual Lab Support for Network Mapping and IP Customization

You can set up a virtual lab in an isolated virtual environment for a VMware destination to perform a test failover operation for a recovery group.

A virtual lab in the isolated network provides the following capabilities:

- Use a network configuration in the virtual lab to mirror the network configuration of the production environment.
- Use a test network mapping to map a source network with an isolated network and VLAN ID to perform a test failover operation.
- Use a masqueraded IP address on the gateway appliance to forward the traffic from the external network to the test failover VMs on the private network.
- Use test VM IP customization and IP masquerading at the VM level, and IP masquerading range at the recovery group level.

More Information

- Periodic Replication Group Options for VMware
- Recovery Target Options for VMware
- Testing Failover for a Periodic Replication Group

Disaster Recovery Is Now Auto Recovery

The Commvault Disaster Recovery (DR) feature is renamed Commvault Auto Recovery.

More Information

- Auto Recovery

Journey To The Cloud

Back Up and Restore Google Cloud BigQuery

You can back up and restore Google Cloud BigQuery projects from the Command Center.

You can perform the following operations:

- Make a full backup
- Restore an entire project
- Restore a dataset or an individual table to the same project from which it was backed up
- Restore an entire project to a different project
- Restore a dataset or an individual table to a different project

More Information

- Google Cloud BigQuery

Linux Access Node Support for Azure SQL

You can use an access node that has a Red Hat Enterprise Linux operating system to back up and restore Azure SQL and Azure Managed SQL instances.

More Information

- System Requirements for Azure SQL Instance
- System Requirements for Azure Managed SQL Instance

Prevent Cross-Region Backups for Azure VMs

You can restrict cross-region backups for Azure hypervisors. The hypervisor's VM groups can still include VMs from different regions, so you can use elastic plans to back up VMs from different regions to region-based storage. Commvault recommends preventing cross-region backups in multi-region environments.

More Information

- Preventing Cross-Region Backups for an Azure Hypervisor

AWS Organizations and AWS Control Tower Support

Commvault supports integration with and protection of AWS environments that are governed by AWS Organizations and AWS Control Tower. AWS Organizations is an account management service that enables AWS customers to consolidate multiple AWS accounts into an organization that they create and centrally manage. AWS Organizations provides centralized control over each account's access to AWS services and API actions, referred to as service control policies (SCPs). AWS Control Tower offers a straightforward way to set up and govern an AWS multi-account environment, following prescriptive best practices. Control Tower applies controls (called guardrails) to ensure that cross-account access permissions are configured according to best practices.

Commvault publishes guidance for customizing your SCPs to ensure that the minimum permissions (often called least privileges) are enabled across your organization for backup and recovery. Additionally, Commvault provides prescriptive guidance about how to configure your Control Tower Account Factory to vend new AWS accounts with the permissions and trust relationships to perform backup and recovery across your organization.

Key Features

- Enable backup and recovery across your organization with resilience-aware SCPs
- Streamline new account protection by vending member accounts with required API actions and cross-account trust
- Speed cyber recovery by ensuring appropriate accounts or organization units (OUs) have cross-account access to perform recovery actions

Applicable Agents

- Virtual Server Agent for Amazon EC2
- Cloud Apps

Setup Requirements

- Verify that you have an AWS Organization and AWS Control Tower created.
- Follow Commvault guidance to enhance your SCPs and Account Factory configuration to prepare your organization for holistic backup and recovery.

More Information

- Requirements and Usage for AWS IAM Policies and Permissions
- What is AWS Organizations?
- What is AWS Control Tower?

Backup and Restore of Azure Cosmos DB Cassandra API Keyspaces and Tables

You can back up and restore Microsoft Azure Cosmos DB accounts that use the Cassandra API. Azure Cosmos DB is a globally distributed, multi-model cloud database (Database-as-a-Service). You can back up and restore Cosmos DB Cassandra API keyspaces and tables across multiple Azure accounts and regions. You can configure full and incremental backups of tables and keyspaces to meet recovery point objectives (RPO), long-term retention, and compliance needs. This functionality is available using the Command Center and REST APIs.

More Information

- Azure Cosmos DB with Cassandra API

Tag Support When Creating VM Groups in Oracle Cloud Infrastructure

When creating a VM group for an OCI hypervisor, you can use tags (created in Oracle Cloud) to create rules that automatically select instances to be included in the VM group.

More Information

- Adding a VM Group for Oracle Cloud Infrastructure

Restore Full Google Cloud Platform Instances to a Different Service Account

When you restore full GCP instances out of place, you can restore the instances to a different service account.

More Information

- Restoring Full Instances Out of Place for Google Cloud Platform

Linux-Based Commvault Cloud in AWS Marketplace

Commvault Cloud (software) running on Red Hat Enterprise Linux is available in AWS Marketplace.

Commvault Cloud is a unified cyber resilience platform that provides unified management, risk governance, threat detection, auto recovery, and cyber recovery. You can deploy your own self-hosted instance of Commvault Cloud (software) inside your Amazon VPC in minutes, using AWS CloudFormation Infrastructure as Code to automate and configure your instance according Commvault and AWS best practice.

Key Features

- Quickly find, test, deploy, and buy Commvault Cloud â€" Foundational Protection (Linux) from AWS Marketplace
- Perform unified cyber resilience management for your AWS and hybrid workloads
- Leverage Linux-based Amazon EC2 compute for 50% reduction in run-time costs from Windows compute
- Hardened OS and application configuration which is actively scanned and updated for vulnerabilities

Applicable Agents

Virtual Server Agent for Amazon EC2

(All Commvault agents are supported by Linux-based Commvault Cloud in AWS Marketplace.)

Setup Requirements

1. Deploy a new Commvault Cloud (software) instance from the AWS Marketplace.
2. Complete initial backup configuration wizards.
3. Start protecting your AWS and hybrid workloads.

More Information

- Linux CommServe: Getting Started with CommServe Server in a Linux Environment
- CommServe Server: System Requirements (Linux)
- Commvault in the AWS Marketplace (PDF)
- Commvault Cloud â€" Foundational Protection in AWS Marketplace

Amazon VPC Cross-Region Recovery and Cloning

Commvault's Amazon VPC recovery, a capability of Amazon EC2 protection, now allows recovery to

alternate Regions and/or AWS accounts. Amazon VPC allows AWS customers to launch AWS resources in a virtual network, which includes subnets, network interfaces, routing, gateways, and service endpoints. Commvault Cloud recovery of Amazon EC2 instances to the original or alternate account and Region is supported. Recovery will automatically discover missing VPC resources and re-create them, allowing cloning of VPCs and enabling non-disruptive disaster recovery testing. Commvault re-creates VPCs, DHCP option sets, Subnets, Security Groups, and Network Interfaces as part of the recovery. Commvault collects configuration of all VPC and related network resources in JSON format for forensic investigations of failed changes or misconfigurations.

Key Features

- Protect Amazon VPC configuration, including subnets, security groups, network interfaces, and tags related to protected Amazon EC2 instances
- Recover Amazon EC2 instances in place, or to an alternate Region and/or AWS account, complete with Amazon VPC configuration that was deleted or modified after backup
- Recover Amazon VPC configuration in JSON format for forensic inspection and analysis as part of incident resolution

Applicable Agents

Virtual Server Agent for AWS

Setup Requirements

Before performing an Amazon EC2 backup and restore (including Amazon VPC resources), update the AWS Identity and Access Management (IAM) policy that is used to protect your Amazon EC2 instances. For the most recent amazon_restricted_role_permissions.json file, see Requirements and Usage for AWS IAM Policies and Permissions.

More Information

- Amazon VPC Resources That Commvault Protects
- Restoring Amazon EC2 Instances and Files
- What is Amazon VPC?

Faster Restores for Amazon S3 Glacier Storage Classes

Commvault software supports improved restore times from Amazon S3 Glacier Flexible Retrieval and Amazon S3 Glacier Deep Archive storage classes. Restores from S3 Glacier storage libraries using the Standard retrieval tier can now use Amazon S3 Batch Operations to achieve up to an 85% improvement in restore time.

Using S3 Batch Operations, you can restore archived data located in Commvault Cloud Storage including Commvault Combined Storage Tier. Multi-object restores occur in parallel to accelerate restore workflows and allow quick response to business data needs. Faster restores powered by S3 Batch Operations is available in all AWS regions, including the AWS GovCloud (US) Regions and China Regions (Beijing, operated by Sinnet; and Ningxia, operated by NWCD).

Key Features

- Improve data restore time from Amazon S3 Glacier Flexible Retrieval by up to 85%, at no additional cost.
- Improve data restore time from Amazon S3 Glacier Deep Archive, at no additional cost.
- Reduce cost of long-term or compliance copies, while achieving accelerated access when required.

Applicable Agents

- IntelliSnap
- Laptop
- Linux File System
- MariaDB
- MySQL
- Oracle
- PostgreSQL
- SQL Server
- Virtual Server for AWS
- Virtual Server for Kubernetes
- Windows File System

Setup Requirements

Ensure that MediaAgent performing the restore is upgraded to Platform Release 2024.

1. Granting Permissions for Amazon S3 Batch Operations
2. Configuring Amazon S3 Glacier Faster Restores
3. Perform a restore

More Information

- Faster Restores for Amazon S3 Glacier
- Cloud Services and Applications Support for Faster Restores
- Combined Storage Tier
- Amazon S3 Glacier Flexible Retrieval improves data restore time by up to 85%
- Reduce recovery time and optimize storage costs with faster restores from Amazon S3 Glacier storage classes and Commvault

Commvault Protects AWS Services in the Israel (Tel Aviv) Region

Commvault protects supported AWS services in the Israel (Tel Aviv) Region, also known as il-central-1. Commvault Cloud provides backup and recovery and autonomous recovery (formerly called Disaster Recovery) for a broad range of AWS compute, containers, database, and storage workloads.

Commvault Cloud provides native AWS snapshot protection and service-independent backup copies for the following:

- Amazon Aurora
- Amazon DynamoDB
- Amazon Elastic Block Store (EBS)
- Amazon Elastic Compute Cloud (EC2)
- Amazon Elastic File System (EFS)
- Amazon Elastic Kubernetes Service (EKS)
- Amazon FSx (all types)
- Amazon Relational Database Service (RDS)
- Amazon Redshift
- Amazon Simple Storage Service (S3)
- Amazon VPC

Commvault Cloud is available in all 32 launched Regions, Local Zones, and Wavelength Zones. Commvault leverages AWS Identify and Access Management (AWS IAM) and AWS Key Management Service (AWS KMS) to securely access, transfer, and store your data within and across AWS accounts and Regions.

Key Features

- Accelerate application migration for applications that require Israel (Tev Aviv) placement for an optimal user experience.
- Run applications with data sovereignty requirements within the Israel (Tel Aviv) geographic region.
- Protect your AWS resources with native AWS snapshots and optional service-independent copies.
- Include Israel (Tel Aviv) in your regional selection based on the sustainability impact, which is part of the shared sustainability model in AWS.

Applicable Agents

Virtual Server Agent for Amazon EC2

Setup Requirements

You can start protecting your applications in the Israel (Tel Aviv) region by upgrading to Commvault Platform Release 2024 and configuring tag-based resource discovery and protection. Commvault will automatically discover and protect your compute, container, database, analytics, and storage workloads using in-region and cross-region snapshots (where supported) and/or service-independent backup copies.

More Information

- Supported AWS Regions and Availability Zones Supported for Amazon EC2 protection
- Commvault Software in the AWS Market Place
- AWS Global Infrastructure
- Now Open - AWS Israel (Tel Aviv) Region

Amazon Linux 2023 Powered Amazon EC2 Protection

You can use Amazon Linux 2023 (AL2023) with AWS Graviton (Arm64) or Intel/AMD (x64) architectures to perform backup and recovery of Amazon EC2 instances. Amazon Linux 2023 (AL2023) is the next generation of Amazon Linux from Amazon Web Services. Develop and run cloud and enterprise applications in a secure, stable, and high-performance runtime environment. With AL2023, you get an application environment that offers long-term support, with access to the latest innovations in Linux. AL2023 is provided at no additional charge. AL2023 is the successor to Amazon Linux 2.
Commvault Cloud access nodes that run Amazon Linux 2023 are available in AWS Marketplace. You can use Commvault Cloud access nodes to auto-scale compute resources during EC2 backups or to perform replication and recovery of EC2 instances.

Key Features

- Improve data-handling security with pre-built SELinux policies and set security policies at boot.
- Simplify operations with frequent minor updates, biannual major updates, and five years of support.
- Adopt AL2023 benefits automatically when using Commvault auto-scaled access nodes for backup (AL2023 will be the default OS for auto-scaling starting in February 2024).

Applicable Agents

Virtual Server Agent for Amazon EC2

Setup Requirements

- Upgrade your Commvault Cloud (CommServe server, MediaAgents, and access nodes) to Platform Release 2024.
- Deploy new Commvault Cloud-Access Node ARM BYOL or Commvault Cloud-Access Node BYOL from AWS Marketplace.
- Assign the newly created access nodes to relevant AWS accounts and VM groups.

More Information

- System Requirements for Protecting Amazon EC2 Instances
- Auto-Scaling for Amazon EC2 Access Nodes
- Commvault Cloud Access Nodes in AWS Marketplace
- What is Amazon Linux 2023? in AWS documentation

Modern Infrastructures

Automatic Access Node Selection for Virtualized Workloads

The Commvault software can automatically select access nodes for managing backups and restores.

When you create a hypervisor, you can select the **Automatic** setting to have the Commvault software automatically select access nodes.

Key Features

- Automatically selects access nodes for managing backups and restores
- Does not require USE PROXY permissions to associate any access node to the company
- Uses the MediaAgents that are associated with your selected plan as access nodes

Applicable Agents

Applicable hypervisors:

- VMware vCenter
- Microsoft Azure (without Managed Service Identity, MSI)
- Amazon Web Services (AWS)
- Nutanix AHV
- VMware vCloud Director

More Information

- Automatic Access Node Selection

WORM lock and retention rules support in Command Center

You can set WORM lock and retention rules for cloud storage and disk storage in Command Center.

More Information

- Defining Retention Rules for Cloud Storage
- Enabling WORM Storage and Retention for Disk Storage
- Defining Retention Rules
- Enabling WORM Storage and Retention for Cloud Storage

Simplified Process to Install Operating System Updates on HyperScale Nodes

You can install operating system updates on the HyperScale nodes using the existing Commvault software update installation process. On HyperScale X nodes, the installation process installs the Commvault Distributed Storage (CDS) updates along with the OS updates.

Setup Requirements

- The CommServe server must have internet connectivity.
- The CommServe and the nodes must be on the same release version and must have Commvault platform release 2022E or later installed.

More Information

- HyperScale X Appliance
- HyperScale X Reference Architecture
- HyperScale 1.5 Appliance
- HyperScale 1.5 Reference Architecture

Security Related Enhancements for HyperScale

The following security related enhancements were made for HyperScale:

- Enable restricted shell on HyperScale clusters to provide an additional layer of security. This process involves the following steps:
  - Creating a 'cvbackupadmin' user with limited capabilities or commands needed to administer the nodes and cluster. This user's capabilities will be limited to the set of commands supported by restricted shell.
  - Disabling root login on the nodes from the Commmand Center, so that only the cvbackupadmin user can log on and access the nodes.
- Enable firewall on HyperScale X clusters, which automatically opens the necessary ports on the HyperScale nodes.

More Information

Enabling Restricted Root Access

- Restricting Root Access on HyperScale X Appliance
- Restricting Root Access on HyperScale Reference Architecture
- Restricting Root Access on HyperScale 1.5 Appliance
- Restricting Root Access on HyperScale 1.5 Reference Architecture

Enabling Firewall

- Enabling Firewall on HyperScale X Appliance
- Enabling Firewall on HyperScale X Reference Architecture

Offline Replication and CIFS Shares Backup and Restore for Azure NetApp Files

You can use Commvault software to back up and restore CIFS shares of Azure NetApp Files volumes using IntelliSnap. The software also allows users to view and monitor the status of the cross-region snapshot replication of the Azure NetApp Files volumes.

Applicable Agents

- Azure NetApp Files

More Information

- Protecting CIFS Shares of Azure NetApp Files Using IntelliSnap
- Offline Replication of Snapshots for Azure NetApp Files

Understand And Activate Data

Monitor File Activity Anomalies for Virtual Machine Guests

Anomalous created, modified, deleted, and renamed file activity insights are now supported for virtual machine guests without requiring an in-guest agent. This provides in-built backup threat monitoring without the complexity of managing and installing agents. This feature utilizes the VM file indexing framework and Commvault's AI/ML engine. This insight may indicate threat activity may have impacted data that was backed up within the VM guest. When anomalies are detected they can be viewed on the Unusual File Activity dashboard, and clean pre-anomalous recoveries can be performed quickly.

More Information

- Unusual File Activity Report for Backup Job Anomalies - Virtual Machine

End-of-Life and Deprecated Features

When a Commvault product or feature has reached End-of-Life (EOL) cycle, full or limited support for the product or feature will be provided from the date of announcement through the date of obsolescence. To view a list of the features, products, and platforms deprecated in this release, see Deprecation Notices.