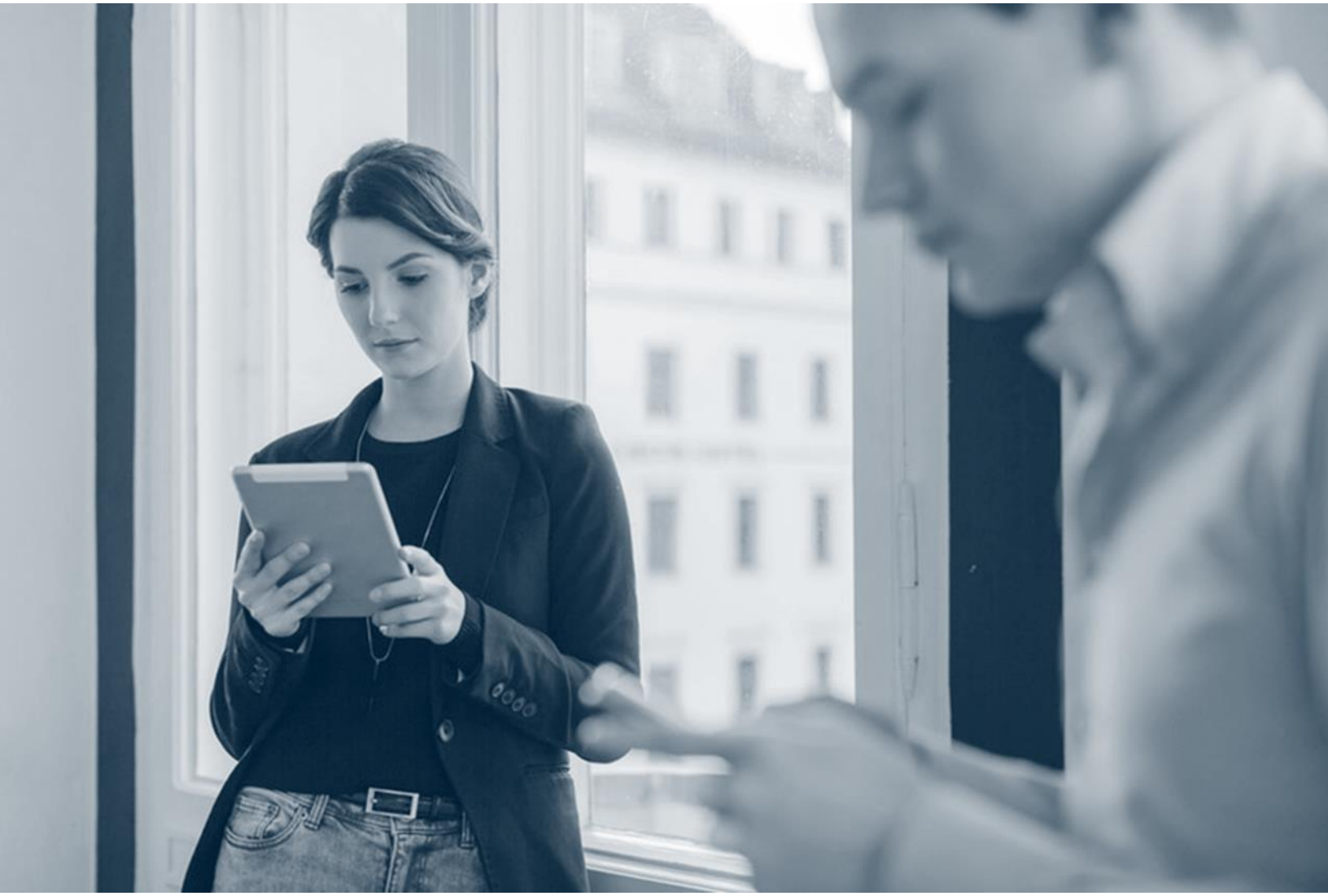
Commvault Platform Release 2023E Newsletter

June 15, 2023



Contents

Complete Backup And Recovery

Download JSON Payload for Command Center Operations

When you perform operations in the Command Center, such as creating a new file server, you can also download the corresponding JSON payload request. You can use the JSON payload request for sending REST API POST requests.

More Information

- Downloading the API JSON Payload for Command Center Operations

Recover All Stubs for a Mailbox (On-Premises and O365)

You can use the stub rehydration method to identify stubs and replace stubs with the original message, even if the stub was moved from one folder to another. You can submit a stub rehydration job to view the summary information about the stubs in a report, to recover stubs, or to update the stub email recall URL.

You can use the stub rehydration feature in all Exchange environment types.

More Information

- Stub Rehydration
- Restoring Exchange Mailbox Using Stub Rehydration

Single SAML Authentication for Tenants the CommCell Level

Service providers can configure SAML authentication at the CommCell level to enable single sign-on for all companies in the CommCell environment.

More Information

- Enabling Single Sign-On for Tenants at the CommCell Level

Message Reply in the Web Console for Exchange Web Services Backup

To use the message "Reply" or "Reply all" feature in the Web Console for Exchange messages that use

EWS (Exchange Web Services) backup, add the Enable Email Web App setting to the CommServe computer.

More Information

- Enabling Message Replies for Exchange Web Services Backup

Secure LDAP Connection for an Active Directory Through a Commvault LDAP Gateway

When the CommServe server or the Web Server does not have direct connectivity to the Active Directory, you can create a secure LDAP connection through a Commvault LDAP gateway.

More Information

- Domain Controller Settings for Active Directory
- Adding Domain Controllers

Webhooks for Alert Notifications

A webhook is a lightweight API that you can use to securely send alert notifications from the Command Center to a third-party application.

The tenant administrators and MSP administrators can configure the third-party application, and then set up the webhook in the Command Center.

More Information

- Adding a Webhook

Performance Enhancements for PostgreSQL File System (Physical, Hot) Based Backups and Restores

Commvault support for protecting an FSBasedBackupSet in PostgreSQL database includes the following enhancements:

- Support for PostgreSQL15.x
- Support for multi-streamed backups
- Support for non-exclusive backup mode

More Information

- PostgreSQL Agent: System Requirements (Command Center)
- Restoring One or More PostgreSQL Databases (Command Center)
- Modifying the Number of Streams for Backups (Command Center)
- PostgreSQL Agent: System Requirements (CommCell Console)
- Performing Restores from FSBased Backup Set (CommCell Console)

Delete SQL Databases

You can delete a database in a SQL instance if you do not need to protect the database. After you delete the database, it is not available for restores.

More Information

- Deleting a SQL Database

File Indexing V2 for Amazon EC2

Starting with Commvault Platform Release 2023E, all indexing-based operations for Amazon EC2 - including backups, snaps, and file indexing - automatically use File Indexing Version 2, providing all the speed, resiliency, and version capabilities that come with this newest indexing scheme.

Existing Amazon EC2 VM groups with File Indexing Version 1 will continue to function with the older indexing scheme. To use File Indexing Version 2 for existing VM groups, simplify modify the VM group's file indexing setting.

More Information

- "Enable File Indexing" in Updating an Amazon EC2 VM Group
- File Indexing Version 1
- File Indexing Version 2

Support for Data Immutability Feature in HPE StoreOnce Catalyst Storage

The Data Immutability feature in HPE StoreOnce Catalyst Storage prevents the backup applications from modifying or deleting StoreOnce Catalyst items during a specific (immutable) period. Additionally, it protects data from accidental deletion and modification through various security attacks like ransomware.

More Information

- Data Immutability Feature

Debugging Workflows in the Command Center

You can debug workflows in the Command Center. In addition, you can search for strings in the workflow to identify activities that need to be modified.

More Information

- Debugging Workflows

Create Custom Backup Categories for Office 365 Applications

You can create custom categories for Exchange Online, OneDrive, SharePoint Online, and Teams backup content so that you can group specific types of content together. This is helpful if you need to have a different backup frequency or require different settings for specific types of backup content.

Key Features

- Use regular expressions to define a set of backup data
- Categorize backup data based on the time when data was created, geographical location, language, user name, and SMTP address (category options vary among applications)

Applicable Agents

- Office 365 Exchange Online
- Office 365 OneDrive
- Office 365 SharePoint Online
- Office 365 Teams

More Information

- Creating Custom Categories for Exchange Backup Content
- Creating Custom Categories for OneDrive Backup Content
- Creating Custom Categories for SharePoint Backup Content
- Creating Custom Categories for Teams Backup Content

Support for Dynamic Credential Retrieval

You can add a third-party credential vault provider in order to secure and manage credentials outside of the Commvault platform. Credentials are retrieved dynamically to perform data protection operations. Dynamic retrieval eliminates the need for users to have direct access to privileged account credentials, so the risk of credential theft, misuse, and cyber attacks is reduced. The credential vault provider might offer additional auditing controls and lifecycle automation policies so that you can audit privileged access and rotate credentials on a regular basis to enhance security without effecting data protection operations. This feature provides a secure and efficient way for organizations to manage privileged account access and remain compliant.

When access to credentials is needed, the credentials are securely retrieved from the third-party credential vault based on how the credentials are mapped within Commvault. Once the backup completes, the credentials are not used by Commvault and are retrieved again only as needed for future backups. Commvault supports CyberArk for dynamic credential management.

More Information

- Adding a Third-Party Credential Vault Provider

Two-Factor Authentication for 1-Touch and Virtualize Me

You can now perform 1-Touch operations on Windows and AIX when two-factor authentication is enabled. For Windows clients, you can also perform Virtualize Me operations when two-factor authentication is enabled.

Key Features

- Virtualize Me
- 1-Touch

Applicable Agents

- Windows
- AIX

More Information

- Performing a Non-Interactive Bare Metal Recovery Using 1-Touch for Windows

IntelliSnap for Nutanix Files

Use IntelliSnap to take snapshots of Nutanix Files data exported as CIFS and NFS shares.

Key Features

- After an IntelliSnap backup operation, perform a backup copy job later at a convenient time.
- Perform a live browse and restore from snapshots of Nutanix Files data.

Setup Requirements

Verify that the following packages are installed on the file server:

- File System Agent
- MediaAgent

More Information

- Nutanix Files

Back Up and Restore InterSystems IRIS in the Command Center

You can back up InterSystems IRIS using the Epic electronic health record (EHR) application.

More Information

- Epic EHR Systems

New Settings Tile for CommCell Entities

The Command Center displays a list of settings that you can configure on a new **Settings** tile, for the following entities in the CommCell environment:

- CommCell
- Company
- Laptop
- MediaAgent
- Server group

More Information

- Configuring Settings for a CommCell
- Configuring Settings for a Company as an MSP Administrator
- Configuring Company Settings (Tenant Administrator)
- Configuring Settings for a MediaAgent
- Configuring Settings for Laptop
- Configuring Settings for a Server Group

Automated Oracle Encrypted Database Backup and Restore

If an Oracle database is encrypted, the Oracle Wallet files are automatically backed up and restored.

Applicable Agents

- Oracle
- Oracle RAC

More Information

- Oracle Wallet Backup and Restore
- Backups for Oracle
- Backups for Oracle RAC

Adding MediaAgent Role for Inactive MediaAgents

You can turn an inactive MediaAgent into an active MediaAgent using the **Add MediaAgent Role** option in the Command Center or the CommCell Console. Active MediaAgents consume a license, while inactive MediaAgents have the MediaAgent package installed, but have not yet consumed a license. When you enable this option, a license is consumed and the MediaAgent becomes active.

More Information

- Adding MediaAgent Role (CommCell Console)
- Adding MediaAgent Role (Command Center)

Optimal Utilization of Dell EMC Isilon/PowerScale Nodes to Back Up CIFS Shares

CIFS backups make better use of the Dell EMC Isilon/PowerScale nodes when the subclient content contains the DNS address of a SmartConnect zone representing multiple Dell EMC Isilon/PowerScale nodes.

More Information

- Optimal Utilization of Dell EMC Isilon/PowerScale Nodes to Backup CIFS Shares

IntelliSnap Support for Hitachi NAS native mode REST API

Commvault now supports Hitachi NAS (HNAS) REST API v7 to perform IntelliSnap operations in 'native' mode. IntelliSnap operations using the previous 'legacy' mode are also supported.

More Information

- Hitachi NAS

Use Region-Based Backups for SAP HANA System Replication

In an SAP HANA system replication setup, if the primary and secondary nodes are located in different workload regions, you can configure the backups to use the storage which is local to the current primary (source) node workload region. Using a region-based plan avoids data transfer over a WAN and enables faster backups and restores.

When the backup job starts from an SAP HANA client, it uses the storage belonging to the workload region defined for the SAP HANA client. If the primary node fails, the secondary node replication client becomes the primary node and takes over the backup operation. In this case, the backup job automatically considers the storage that is defined in the plan based on the workload region.

When a multi-region server plan is assigned to an SAP HANA non-replication instance, the backup job will automatically select the storage based on the workload region defined for the server.

Applicable Agents

SAP HANA

More Information

- Using Region-Based Backups for SAP HANA System Replication
- Creating a Server Plan
- Assigning a Workload Region to an Entity

Complete: Enable Service Providers

Back Up and Restore vApp Templates from VMware Cloud Director

You can back up and restore vApp templates from VMware Cloud Director.

This feature supports a rule-based discovery of catalogs and VM templates.

Setup Requirements

A VM group must be created to include vApp Templates.

More Information

- Adding a VM Group for VMware Cloud Director
- Managing VM Group Content for VMware Cloud Director
- Performing Backups for VMware Cloud Director VMs or VM Groups
- Restoring vApp Templates for VMware Cloud Director

Backup and Restore of Standalone VMs in an Organization Virtual Datacenter

You can perform full backups and restores of standalone VMs in an Organization Virtual Datacenter (Org vDC) starting with VMware Cloud Director 10.3.0.

In the Commvault software, the restore dialog box has a "Restore as Standalone VM" option that you can use to restore a VM as a standalone entity within the Org vDC.

Key Features

Backups and restores of standalone VMs in the Org vDC

Applicable Agents

Virtual Server Agent

More Information

- Restoring Full Virtual Machines for VMware Cloud Director

View Growth and Trends and Workload Usage in the Licensing Reports

Information about license usage by workload has been added to the licensing reports. Additionally, growth and trends information has been added to these reports, which shows license usage over time. This information can help you view license usage trends and estimate license usage in the future, including whether you need to purchase additional licenses.

More Information

Workload Usage

- Workload Summary in the License Summary Report
- Current Workload in the License Summary Worldwide Report
- Data Views for the Subclient Peak Usage Report: Workload Usage Tabs
- Workload Summary for a Single CommServe Computer
- Workload Summary in the License Server Usage Summary Report

Growth and Trends

- Growth and Trends in the License Summary Worldwide Report

VMware Cloud Director 10.4 Backup, Restore, and Plugin Support

You can use VMware Cloud Director Version 10.4 for backups, restores, and plugin configuration. VMware Cloud Director 10.4 is supported in 11.28 and more recent releases.

More Information

- VMware Cloud Director
- Commvault Plug-In for VMware Cloud Director

Complete: Manage New Workloads

Multiple Access Node Backups for Object Storage

Cloud and object storage backup uses a simple and scalable multi-node architecture that increases performance and adds high availability to meet RPOs and RTOs for large data sets.

Setup Requirements

Access nodes must be of similar operating system type.

More Information

- Adding an Alibaba Object Storage Service Repository
- Add the Object Storage Repository for Amazon S3
- Configuration for Azure Blob Storage
- Add the Object Storage Repository for Azure Data Lake Storage Gen2
- Adding an Azure File Storage Object Storage Repository
- Adding a Google Cloud Object Storage Repository with an Access Key and a Secret Key
- Adding IBM Cloud Object Storage Repository
- Adding an Oracle Cloud Infrastructure Object Storage Repository

Use Self-Service for Exchange Online and OneDrive for Business to Manage Backups

You can use the Self-Service feature to manage archived messages and files from Exchange Online and OneDrive for Business. Messages from your Exchange Online mailbox and files and folders from your OneDrive appear in the Command Center where you can find, view, and restore them.

Key Features

Exchange Online

- View, export, and restore messages to your Exchange Online mailbox
- Search for specific messages or attachments
- Download copies of emails

OneDrive for Business

- View, export, and restore files and folders to your OneDrive
- Search for specific files
- Download copies of files and folders

More Information

- Exchange Online Self-Service
- OneDrive for Business Self-Service

Transform Kubernetes API resources During Restore and Migration

Commvault software supports dynamic Kubernetes API resource transformation during application recovery and migration. Using the Kubernetes API, you can query and manipulate API resources and objects (such as Pods, Namespaces, ConfigMaps, and Events). You can modify (add, delete, or modify) your applications API resources during a restore, allowing customization to match your target cluster or

environment. Resource modification is crucial when performing cloud-native application mobility, cloning, or disaster recovery.

Commvault extended the Kubernetes API with a CustomResourceDefinition that describes a new custom resource of kind RestoreModifier. You can manage a library of reusable RestoreModifiers to transform your applications' metadata (labels, annotations), network (services, ingresses, routes), and security configuration to meet your business rules. To do this, select the RestoreModifiers when restoring across clusters, geographies, or namespaces, and then Commvault transforms the resources before creating them on your cluster.

Key Features

- Transform application resources during migration and cloning across clusters, geographies, and namespaces.
- Simplify cloud-native Disaster Recovery by dynamically transforming applications for the destination cluster or location.
- Automate at scale by automatically applying labels and annotations to ensure cost transparency and secure operations.

Applicable Agents

Virtual Server Agent for Kubernetes

Setup Requirements

- Update the CommServe server, MediaAgents, and Kubernetes access nodes to Platform Commvault Release 2024.
- Define one or more RestoreModifiers during a full application restore.
- Perform a full application or namespace restore and apply the RestoreModifiers in the Advanced Options section.

More Information

- Creating Reusable Resource Modifiers for Kubernetes
- Automatically Modifying Kubernetes Applications During Restores
- Custom Resources (in the Kubernetes documentation)
- CustomResourceDefinitions (in the Kubernetes documentation)

Complete: Protect Virtual Environments

Restore VM Disks with End User Attach Disk Restore Support for VMware, Azure, OpenStack; Select Datastores at the Disk Level for VMware Full VM Restores

For VMware, Azure, and Open Stack, users can restore a virtual machine disk to an existing VM. The disks are restored and attached to the destination VM.

For VMware, during a full VM restore, users can select the datastore for each disk associated with the VM.

More Information

VMware:
- Restoring a Full Virtual Machine Out of Place for VMware
- Restores for VMware
- Attaching a Disk to an Existing VM for VMware

Azure:
- Restoring Azure VMs and Files
- Attaching a Disk to an Existing VM for Azure

Open Stack:
- Restores for OpenStack
- Attaching a Volume to an Existing OpenStack Instance

Configure Backup Type and Disk Filters for Individual VMware VMs

For VMware VMs that use indexing V2 and streaming backups, you can specify the backup type and disk filters for individual VMs without creating separate VM groups.

Key Features

- You can override the VM group settings and change the backup type for individual VMs in the VM group.
- You can configure disk filters for individual VMs and also include or exclude the VM group disk filters for the VM backups.

Applicable Agents

Virtual Server Agent

More Information

- Creating a Disk Filter for VMware VM
- Modifying the Backup Type for a VMware VM

Application-Consistent Snapshots for Azure VMs

You can use the new "File system and application consistent" backup type for Azure VMs to perform a

point-in-time application-consistent snapshot of all the managed disks of the VM.

Applicable Agents

Virtual Server Agent for Microsoft Azure

More Information

- See "Modify the Backup Type" in Updating an Azure VM Group

Select Destination Key Vault for Restores of ADE-Encrypted VMs

When you restore VMs that are encrypted with Azure Disk Encryption (ADE), you can select the Key Vault to encrypt the VM with.

Applicable Agents

Virtual Server Agent for Azure

More Information

- Restoring a Full Azure Virtual Machine Out of Place

Kubernetes, Azure, and AWS Virtualization Onboarding via Terraform

New Terraform resources are now available to aid in onboarding Kubernetes, Azure, and AWS workloads. Other supporting Commvault resources such as plans, credentials, and storage are also available to simplify the onboarding experience. These resources are documented in the Terraform registry.

More Information

- Resources for the Commvault Terraform Module

ARM Access Nodes for Azure VMs

With the introduction of ARM-based processors in Azure, you can use this new VM type for your Commvault access nodes for cost-effective and energy-efficient infrastructure.

Applicable Agents

Virtual Server Agent for Azure

More Information

- Protecting Azure Virtual Machines with Commvault

Azure Application Security Groups Are Retained with Restores to the Same Network

During Azure VM restores, application security group (ASG) associations are retained if the VM is restored to the original Virtual Network that contains the ASG.

More Information

- Backing Up Azure VMs

Multiple Region Support for Oracle Cloud Infrastructure (OCI) Hypervisors

You can select one or more regions when creating an Oracle Cloud Infrastructure (OCI) hypervisor.

More Information

- Adding an Oracle Cloud Infrastructure Hypervisor
- Adding a VM Group for Oracle Cloud Infrastructure
- Restoring Full Instances for Oracle Cloud Infrastructure

Restore Azure VMs from IntelliSnap Backups by Attaching a Disk to an Existing VM

You can restore Azure VMs from IntelliSnap backups by attaching a disk to an existing VM. (The ability to perform this type of restore for streaming backups is already supported.)

Some limitations exist, such as that you cannot perform this type of restore for unmanaged disks from IntelliSnap backups.

Applicable Agents

Virtual Server Agent for Microsoft Azure

More Information

- Attaching a Disk to an Existing VM for Azure

Back Up and Recover VMs Using vCenter Server 8.0

You can protect and restore VMs from vCenter Server version 8.0 with the Commvault software.

VDDK7.X, which ships with Commvault Platform Release 2022E (11.28) and 2023 (11.30), can protect vSphere 8 managing VMs.

More Information

- VMware System Requirements (Command Center)
- System Requirements for Virtual Server Agent with VMware (CommCell Console)

Protecting Azure ARM VMs

With the introduction of ARM-based processors in Azure, you can protect this new VM type with the Commvault software.

Applicable Agents

Virtual Server Agent for Microsoft Azure

More Information

- Now in preview: Azure Virtual Machines with Ampere Altra Arm-based processors on the Azure website
- Protecting Azure Virtual Machines with Commvault

VM Centric Operations for Nutanix AHV

You can use Commvault VM-Centric operations for Nutanix AHV VMs.

More Information

- Hypervisor Support for VM-Centric Operations

Disaster Recovery

Auto Recover VMs to Nutanix AHV Destinations

You can replicate Nutanix AHV VMs to Nutanix AHV destinations using the Auto Recovery feature. With Nutanix AHV recovery groups, you can perform failover and fallback operations.

More Information

- Creating a Recovery Group Using the Recovery Configuration Tool

Undo Failover Support for Azure

Undo failover support for Azure reduces the time required to switch from DR to the primary site and enables you to discard changes on the DR VM. Undo failover is supported only for managed DR VMs.

With the ability to undo failover for Azure, 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.

After the failover, staging blobs are retained and you can enable or disable undo failover support for Azure during failover operations.

More Information

- Undoing a Failover

Hyper-V Failback Support

Hyper-V Failback is supported for Windows 2016 or higher.

Failback enables you to recover systems and restore them to their original states after failover events. It helps to ensure continuity of business, allowing you to resume operations as quickly as possible after a disaster. Failback also helps to preserve data integrity. You can verify that your data is not lost,

corrupted, or interrupted during a failover event, even if it persists for an extended period of time.

The process is straightforward. A pair of virtual machines are replicated and periodically synchronized. When a failover occurs, the secondary VM of the pair becomes the production copy. When a failback is requested, the pair is brought back in sync with the newest updates from the secondary VM and recovering the primary VM. After that, the pair resumes in their original order and the primary VM resumes production.

More Information

- Performing a Failback for a Periodic Replication Group

Replicate Hyper-V VMs to VMware Destinations

Replicate Hyper-V source VMs to VMware destinations using a replication group. Use the Replication Monitor to track replication operations and perform other operations such as failover and undo failover.

More Information

- Creating a Recovery Group Using the Recovery Configuration Tool

Reuse an Existing AWS Destination Instance During an Incremental Replication

In-place incremental replication jobs to AWS reuse an existing destination instance, rather than deleting the existing destination instance and creating a new instance for each incremental replication job.

Key Features

- Cost savings due to reduced instance runtime.
- Quicker replications because instance creation and deletion steps are skipped.
- Creation of a network interface controller (NIC) for the new destination instance, for each incremental replication job, is not needed.

Applicable Agents

- Virtual Server Agent for AWS

More Information

- Considerations for Amazon Auto Recovery
- Auto Recovery Process using Amazon EBS Direct APIs
- Replication Using the HotAdd Restore Method

Journey To The Cloud

Delete Backed-Up Data for OneDrive for Business, SharePoint Online, and Teams

To reduce backup capacity, you can permanently delete backed-up data so that it is no longer included in backups and cannot be restored. You might also want to permanently delete data for legal purposes and to adhere to compliance regulations.

Key Features

You can delete the following types of data:

- All data for a user
- Specific files, folders, and other items
- Items that match search criteria

Applicable Agents

- OneDrive for Business
- SharePoint Online
- Teams

More Information

- Deleting Backed-Up Data for OneDrive for Business
- Deleting Backed-Up Data for SharePoint Online
- Deleting Backed-Up Data for Teams

Forever Incremental Backups for Oracle Databases Hosted on AWS or Azure

For large Oracle databases hosted on AWS or Azure that cannot finish full backups on weekends or during a desired backup window, you can use this feature to provide forever incremental backups. The feature makes incremental backups by using snapshot creation of Amazon EBS volumes or of Azure managed disks, along with using AWS and Azure block change tracking APIs.

Applicable Agents

Oracle

More Information

- Forever Incremental Backups for Large Oracle Databases Hosted on AWS or Azure

Live Mount for Hyper-V Hosted on Azure

Using Live Mount, you can use nested virtualization to run a Hyper-V virtual machine directly from a backup stored on Microsoft Azure.

More Information

- Live Mount for Hyper-V Hosted on Azure

Open Replication with NetApp SnapMirror Cloud

NetApp Open Replication with SnapMirror Cloud replicates snapshots from a storage virtual machine to a NetApp-supported object storage destination.

Key Features

- NetApp Open Replication

More Information

- NetApp Open Replication with SnapMirror Cloud

Restore Guest Files and Folders from IntelliSnap Backups for Google Cloud Platform

You can restore guest files and folders from an IntelliSnap backup of a Google Cloud Platform (GCP) instance to a specified destination (access node).

Key Features

Commvault supports browsing and recovering of individual guest files on virtual machines. This new feature extends this capability to snapshot backups in GCP. You can quickly search for, access, and recover files from existing snapshots, which can be useful for managing large-scale datasets.

Applicable Agents

Virtual Server Agent for Google Cloud Platform

Setup Requirements

IntelliSnap backup of a GCP instance

More Information

- Restoring Guest Files and Folders for Google Cloud Platform

Enhanced Commvault Protection for Amazon Virtual Private Cloud (VPC)

Commvault's Amazon VPC recovery, a capability of Amazon EC2 protection, now protects and re-creates additional VPC resources. Amazon VPC allows AWS customers to launch AWS resources in a virtual network, which includes subnets, network interfaces, routing, gateways, and service endpoints.

Amazon VPC recovery now re-creates VPCs, subnets, security groups (including security groups), and network interfaces. Additionally, forensic configurations such as DNS attributes, Network Address Usage (NAU) metrics, Delete on termination preferences, sourceDestCheck preferences, IPv4 prefixes, custom IPv4 addresses, MapPublicIpOnLaunch preferences, and DHCP option sets is recoverable, helping operations teams more quickly recover the business. Additionally, customer gateways and VPN connections are collected for forensic investigation of changes.

Recovery of individual Amazon EC2 instances to the original account and Region, along with some dependent VPC resources is supported.

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, 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 Amazon Web Services (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
- What is Amazon VPC?

Back Up and Recover Amazon Aurora, Amazon RDS, and Salesforce by Using AWS Graviton

Commvault software has expanded its AWS Graviton-powered data management to include Amazon Aurora, Amazon RDS, and Salesforce protection. Amazon Aurora, Amazon RDS, and Salesforce service-independent backup and recovery can now be performed with AWS Graviton-based Amazon EC2 instances. AWS Graviton provides the best price per performance of any general-purpose compute option while delivering the highest performance per watt, helping you build more sustainable solutions in AWS.

With this release, Commvault performs export-based backup and recovery of Amazon Aurora (MySQL, PostgreSQL), Amazon RDS (MySQL/MariaDB, PostgreSQL, and Oracle). and Salesforce, using AWS Graviton-powered instances. AWS cloud database dump or export-based protection performs a database-native dump to provide service-independent backups that may be used for long-term retention or database mobility. This approach delivers the best price per performance for data management while using the most sustainable general-purpose compute option available in Amazon EC2. AWS Graviton-powered protection is supported in the AWS Regions, AWS Local Zones, and AWS Outposts that provide Graviton-based EC2 instances.

Commvault Graviton-powered data management now protects Amazon Aurora, DocumentDB, DynamoDB, EC2, EBS, EFS, FSx, RDS, RDS Custom, Redshift, S3, VPC, Workspaces, and AWS Local Zones, Outposts, and Wavelength Zones.

Key Features

- Protect and recover Amazon Aurora, Amazon RDS, and Salesforce instances with AWS Graviton-based instances, which deliver up to a 40% better price-performance ratio over comparable x86 EC2 instances. For more information, go to "Benefits" on the Amazon AWS Graviton Processor website.
- Create long-term retention, compliance, and service-independent copies of your Amazon Aurora, Amazon RDS, and Salesforce instances on Amazon S3.
- Meet your shared sustainability responsibility and carbon reduction goals by leveraging Graviton instances that use up to 60% less energy than comparable EC2 instances. For more information, go to "Benefits" on the Amazon AWS Graviton Processor website.

Applicable Agents

Amazon Aurora

- MySQL
- PostgreSQL
- Virtual Server for Amazon Web Services (AWS)

Amazon RDS

- MariaDB
- MySQL
- PostgreSQL
- Virtual Server for Amazon Web Services (AWS)

Salesforce

- Cloud Apps

Setup Requirements

1. Deploy at least one AWS Graviton access node using the Commvault Cloud Access Node ARM BYOL AWS Marketplace Image. The Cloud Apps and Virtual Server packages are included.
2. Push install the MariaDB, MySQL, and/or PostgreSQL agents to the access node.
3. Configure protection of the Amazon Aurora and/or Amazon RDS database (export-based backup) and/or Salesforce instances and select the newly deployed AWS Graviton access node or nodes.
4. Perform a test backup and restore.

More Information

Commvault

- Amazon Aurora - Export-based backup
- Amazon RDS for MySQL - Export-based backup
- Amazon RDS for PostgreSQL - Export-based backup
- Amazon RDS for MariaDB - Export-based backup
- Salesforce Access Node: System Requirements
- Deploying a Commvault Access Node from the AWS Marketplace

Amazon

- AWS Graviton Processor
- AWS Well-Architected Framework - The shared responsibility model

Application-Integrated Protection for Amazon RDS Custom Databases

You can protect and recover Amazon RDS Custom for Oracle databases and Amazon RDS Custom for SQL Server databases with Amazon RDS native snapshots, database exports, and application-integrated streaming backups. The kinds of protection you can use depend on whether the Commvault agent is installed on the Amazon RDS compute instance or on the access node.

Amazon RDS Custom is a fully managed database service for business applications that require customization of the database and/or operating system.

You can perform full database instance backup and recovery using the following methods:

- Amazon RDS snapshot backups: Commvault IntelliSnap ensures that you can quickly recover your very large databases (VLDBs) by using Amazon RDS snapshots within the same AWS Region.
- Commvault database-native exports: These exports provide a service-independent full copy of your database for long-term retention or compliance needs.

Alternatively, you can achieve granular point-in-time recovery by installing database agents on your Amazon RDS compute instances. These database agents capture database transaction logs and configuration settings. You can recover your database instances rapidly by simply performing a database roll-forward or rollback. Commvault protects Amazon RDS Custom databases in all supported AWS Regions, including GovCloud (US). By default, backups are encrypted during transmission (data in transit) and at rest (data at rest).

Key Features

- Protect your Amazon RDS Custom databases by using RDS snapshots within and across AWS Regions and accounts.
- Create service-independent, application-aware streaming backups of your Amazon RDS Custom databases (Oracle and SQL Server).
- Perform point-in-time full or accelerated partial recovery of Oracle databases, including individual tablespaces, data files, archive logs, control files, and SPFILEs.
- Perform an Oracle RMAN duplicate recovery to a specific point-in-time or a specific Oracle system change number (SCN).
- Perform point-in-time full or accelerated partial recovery of SQL Server databases, including individual tables, data files, and transaction log files.

Applicable Agents

- Oracle
- SQL Server
- Virtual Server for Amazon Web Services

Setup Requirements

1. Upgrade your CommServe computer, MediaAgents, and then access nodes to Commvault Platform Release 2023E.
2. If you will be using an in-guest agent, install the Commvault Oracle or Microsoft SQL Server agent on your Amazon RDS instance. Otherwise, install the agent and cloud apps on the access node.
3. Initiate a backup.

More Information

- Amazon RDS Custom for Oracle
- Amazon RDS Custom for SQL Server

Credential Manager for Google Cloud Platform Instances

You can use Commvault's Credential Manager to save and edit Google Cloud Platform (GCP) hypervisor credential entities. These credentials can be re-used with multiple GCP hypervisors.

Applicable Agents

Virtual Server Agent for Google Cloud Platform

More Information

- Configuring Backups for Google Cloud Platform Instances

ARM Access Nodes for Google Cloud Platform Instances

You can use ARM-based VMs for your Commvault access nodes, for cost-effective and energy-efficient infrastructure.

Applicable Agents

Virtual Server Agent for Google Cloud Platform

More Information

- Protecting Google Cloud Platform Instances with Commvault

Commvault Protects United Arab Emirates, Zurich, Spain, Hyderabad, and Melbourne AWS Regions

Commvault offers backup and recovery support for the 27th (Middle East, UAE), 28th (Europe, Zurich), 29th (Europe, Spain), 30th (Asia Pacific, Hyderabad), and 31st (Asia Pacific, Melbourne) AWS Regions. Commvault supports protection for all 31 AWS Regions, 99 Availability Zones, 32 Local Zones, and 29 Wavelength Zones. The new regional support provides Amazon-native snapshot protection and service-independent backup copies for a broad range of AWS services.

Commvault also protects and recovers Amazon EC2, Amazon Aurora, Amazon DynamoDB, Amazon EBS, Amazon RDS, Amazon Redshift, Amazon VPC, and Amazon S3 resources in the new regions. Data is always kept secure with integration with AWS Identify & Access Management (AWS IAM) and AWS Key Management Service (AWS KMS).

Key Features

- Accelerates application migration to AWS Cloud into any of the launched 31 AWS Regions.
- Runs applications with data residency requirements to run and securely store data within a geographic region.
- Protects your AWS resources with native snapshots and optional service-independent copies in regions and across regions.
- Leverages AWS Global Infrastructure to deploy Commvault Backup & Recovery in a resilient, scalable, and secure manner.
- Selects AWS Regions on their sustainability impact, which is described at Amazon sustainability.

Applicable Agents

Virtual Server Agent for Amazon Web Services

Setup Requirements

You can start in the Middle East, Zurich, Spain, Hyderabad, and Melbourne regions by upgrading to Commvault Platform Release 2023E and configuring tag-based resource discovery and protection. Commvault will discover and protect your compute, database, and storage workloads using in-region and cross-region snapshots and/or Amazon S3 backup copies.

More Information

- Supported AWS Regions and Availability Zones
- Commvault Software in the AWS Market Place
- AWS Global Infrastructure

Protect Google Cloud Platform ARM Instances

You can protect Google Cloud Platform instances that use an ARM-based processor with the Commvault software.

Applicable Agents

Virtual Server Agent for Google Cloud Platform

More Information

- Protecting Google Cloud Platform Instances with Commvault

Modern Infrastructures

Enhancements for Installing Operating System Updates on HyperScale Nodes

The following enhancements improve the process for installing operating system (OS) updates on HyperScale nodes:

- Size-optimized OS update package: In environments where the CommServe server has no internet connectivity, you can download and install OS updates on the Hyperscale nodes using a size-optimized package named metadata.tar. This installation process is simpler and quicker because it does not require downloading the complete OS update packages that are needed for the upgrade.
- Perform parallel operating system upgrades on HyperScale 1.5 Appliance and reference architecture: OS updates can be installed in parallel on horizontally scaled storage pools that have multiple blocks. This parallel update installation process keeps the turnaround time for performing

OS upgrades to a minimum by exploiting the resiliency provided by multiple blocks of nodes.

More Information

Installing OS updates using a size-optimized package

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

Performing parallel OS upgrades

- HyperScale 1.5 Appliance
- HyperScale 1.5 Reference Architecture

Non-Disruptive OS Upgrades for HyperScale X

To ensure uninterrupted operations, Commvault Distributed Storage (CDS) updates can now be upgraded non-disruptively.

More Information

- Installing Operating System Updates on HyperScale X Appliance
- Installing Operating System Updates on HyperScale Reference Architecture

Visit the Commvault Documentation website for complete documentation of Commvault products.