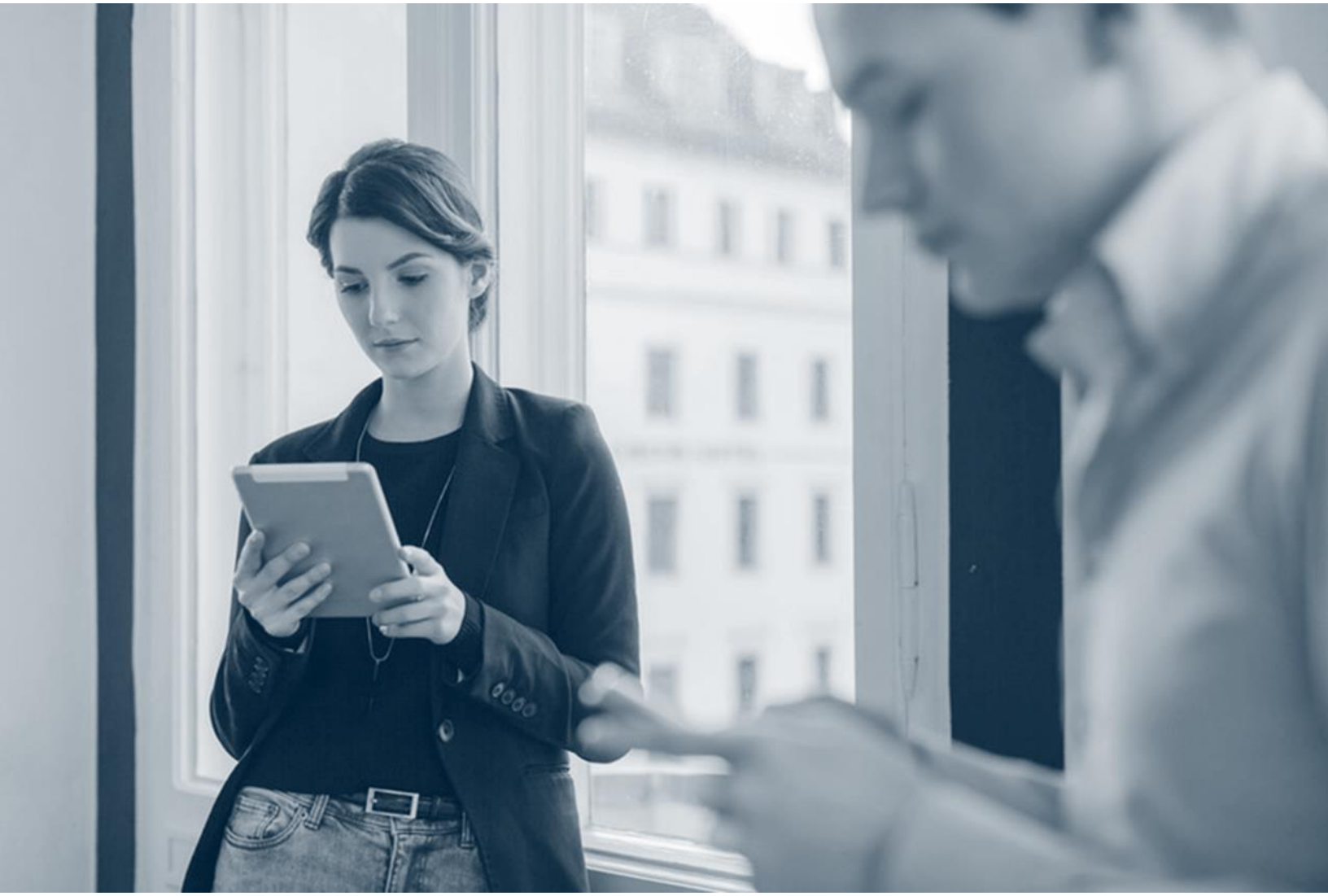
COMMVAULT

Commvault Platform Release 2022E Newsletter

June 15, 2022



Contents

Complete Backup And Recovery

Improved Scalability of Data Verification Operations on Deduplication Databases

Scalability of data verification operations is enhanced to allow greater concurrency across horizontally scaled DDBs. Job batching during data verification is also introduced to further optimize the use of CommServe server resources.

More Information

- Performing a Data Verification Operation on Deduplicated Data

Space Reclamation for Cloud Storage

You can run space reclamation operations to reclaim free space on deduplicated cloud mount paths.

More Information

- Performing a Space Reclamation Operation on Deduplicated Data

Multi-CommCell Installation Routing Using Command Center Endpoint URL

In multi-CommCell or multi-tenant environments with web service routing, you can configure one URL to be the single entry point for users to access their web services.

Key Features

Client installations can be performed by providing an endpoint URL instead of a gateway/server, which reduces the need to host multiple packages.

More Information

- Multi-CommCell Installation Routing Using Command Center Endpoint

Detect File Type Anomalies in Backups

Files with a file type that is different from the file extension or that is invalid due to potential corruption are detected and listed in the Unusual File Activity dashboard as a File Type anomaly.

The file type discrepancies could be malicious in nature, or could indicate some other destructive activity on the system. When the number of file type anomalies exceeds 10% of the total files protected in a backup job, the software sends an alert to the administrator and displays an event message. These files can be viewed in the Unusual File Activity report. From this report, you can mark the file safe, download the file in its infected form for forensic purposes, or recover a previous good version of the file that was protected in previous backups automatically.

More Information

- Unusual File Activity Report for File Type Anomaly Detection in Backup Jobs

Associating Server Plans with Subclients Using Plan Rules

You can assign a server plan by using a plan rule to discover subclients that do not have a server plan or a storage policy. Plan rules contain criteria that determine which server plan to assign to a subclient. You can specify whether to assign plans manually or automatically.

More Information

- Plan Rules

Configure WORM Storage

You can use WORM (write once read many) storage for both deduplicated and non-deduplicated data in both disk and cloud environments.

For cloud platforms that support object-level retention, the Commvault software uses object-level locking. For other cloud platforms, Commvault uses bucket-level or container-level locking.

To configure WORM storage in Commvault, you use a workflow that automatically configures all required settings for WORM storage.

More Information

- Configuring WORM Storage Mode on Cloud Storage
- Configuring WORM Storage Mode on Disk Libraries

Configure Media Management Parameters from the Command Center

You can configure the most commonly used Media Management parameters from the Command Center through the Additional Settings configuration.

More Information

- Media Management Configuration Parameters

Restore Oracle and Oracle RAC Tables in the Command Center

You can restore Oracle and Oracle RAC tables using the Command Center.

More Information

- Restoring an Oracle Table to Its Current Location (In Place)
- Restoring an Oracle Table to a Different Location (Out of Place)
- Restoring an Oracle RAC Table to Its Current Location (In Place)
- Restoring an Oracle RAC Table to a Different Location (Out of Place)

Access a File System Backup from a Windows Computer as an SMB Share

From a Windows computer, you can access a file system backup as an SMB share (that is exported from a Windows MediaAgent) to perform data operations such as the following:

- Threat detection and scanning
- Analytics of the backup data
- Backup validation

Setup Requirements

The Dokany package is installed automatically when the user creates a 3DFS share for the SMB protocol.

More Information

- Getting Started with 3DFS

Logging On to the CommCell Console with a Browser

You can use SAML based Identity Providers (such as Active Directory Federation Services, Azure Active Directory, or Okta) to authenticate the CommCell Console through a web browser. This feature allows you to use modern authentication protocols across all of the Commvault interfaces such as the CommCell Console and the Command Center.

More Information

- Opening the Stand-Alone CommCell Console
- Opening the CommCell Console with a JAR File

Server Plan RPO Schedule Enhancements

With the server plan RPO schedule enhancements, you can now:

- Add additional full, differential, and incremental backup schedules to the existing default incremental backup schedule of a server plan. The most frequent backup schedule is considered to be the RPO of the server plan.
- Delete all backup job schedules associated to a server plan. Such server plans without any RPO can be used for on demand backups.
- Associate a new time zone to the server plan. The backup schedules will run at the same time according to the new time zone for all the servers irrespective of the location of the servers.
- Optionally, add exceptions for specific days of the month or specific weeks in a month during which backup jobs should not run.

More Information

- Creating a Server Plan
- Modifying a Server Plan
- Configurations for RPO

Use Your Own Key for Encryption

By default, Commvault manages the creation and usage of encryption keys. You can also manually generate your own encryption keys outside of Commvault, import them into an external Key Management Server (KMS), and use them for data encryption in Commvault. When bringing your own keys, you must create one key for each storage pool.

More Information

- Managing a Key Management Server

WinPE ISOs for Windows 1-Touch

The 1-Touch ISO is upgraded to WinPE 8.1 to better support newer hardware and versions of Windows.

More Information

- 1-Touch ISOs

Restore Teams Posts

Microsoft Teams chat can be restored as an HTML file for offline review. You can also restore a Teams chat back in place.

More Information

- Restores for a Team in Teams in Command Center documentation
- Restores of Teams Items in Teams in Command Center documentation
- Restores for a Team in Teams in Metallic documentation
- Restores of Teams Items in Teams in Metallic documentation

View License Usage for All Virtual Workloads Under Virtual Operating Instances

You can monitor license usage for all virtual workloads, including Kubernetes, under the simplified view of Virtual Operating Instance (VOI) in the License Summary Report, the License Summary Worldwide Report, the Subclient Peak Usage Report, and the Company Usage Report.

More Information

- License Summary Report (LSR)
- License Summary Worldwide Report
- Subclient Peak Usage Report (SPUR)
- Company Usage Report

Commvault Supports CIS Level 1 Security for Linux CommServe

The Commvault software supports the CIS Level 1 security controls in the following benchmarks for a Linux CommServe:

- CIS Microsoft SQL Server 2019 Benchmark v1.2.0 for the SQL Server Deployed in a Linux Environment
- CIS Red Hat Enterprise Linux 8 Benchmark v1.0.1

More Information

- Certifications and Compliance

Validate IntelliSnap Backups of Application Data for VMware

You can validate IntelliSnap backups of VMware guest virtual machines, including VMs that run applications. Validation performs a live mount operation for the VM and can leverage scripts to verify that the VM and application are usable.

You can use validation to verify that backups are available if you need to restore application data from a backup, or to replicate VMs and applications for use in the event of a disaster.

More Information

- Application Validation for VMware VMs

Complete: Enable Service Providers

Resource Pools For Managing Infrastructure

Resource pools are useful for managed backup service providers (MSPs) that provide Office 365 (Exchange Online, OneDrive For Business, SharePoint Online, Teams), Azure AD, and Dynamics 365 backup services to their tenants using Office 365.

An MSP administrator can use a resource pool to map all the infrastructure details that are needed for the Office 365 apps to the storage pool. Then the tenant administrator can create the Office 365 apps using minimum details.

More Information

- Resource Pools for Managing Infrastructure

Complete: Manage New Workloads

Back Up and Restore Entire Kubernetes Clusters and Namespaces

Commvault now protects entire Kubernetes clusters including all cluster-scoped and namespace-scoped resources. Cluster-scoped resources are part of your Kubernetes cluster configuration and can be used by one or more of your Kubernetes applications. Commvault collects all cluster-scoped resources and allows recovery of all or selective cluster-scoped resources separately from application recovery. Additionally, Commvault expanded its existing application-centric protection to include entire namespace protection. Applications can consist of directly referenced and indirectly referenced (orphaned) resources located within a namespace. Commvault collects all namespace-based resources, which ensures that your Kubernetes workloads are fully protected and recoverable.

Commvault provides complete protection for all your Kubernetes resources, allowing operational recovery, application migration, and disaster recovery across your hybrid Kubernetes landscape. Commvault supports all CNCF Kubernetes distributions, and provides storage snapshot-based protection for both CSI-enabled StorageClasses and direct vCenter snapshot integration with VMware vSphere Cloud Native Storage (CNS).

Key Features

- Protect your entire Kubernetes cluster, including cluster-scoped and namespace-scoped resources
- Protect Kubernetes applications (workload resources) and persistent volume data, including referenced and orphaned objects
- Protect Persistent Storage volumes that reside on Container Storage Interface (CSI) controlled StorageClasses
- Protect VMware vSphere Cloud Native Storage (CNS) volumes via direct snapshot integration with vCenter
- Restore single or multiple applications (namespaces) or all cluster resources to original or to another cluster

Applicable Agents

Virtual Server Agent for Kubernetes

Setup Requirements

- Verify that your Kubernetes application group has the **Full cluster** check box selected.
- Perform application group backups as you normally do.

More Information

Commvault documentation:

- Protecting Kubernetes with Commvault: Data You Can Back Up
- System Requirements for Kubernetes
- Creating an Application Group for Kubernetes
- Restoring Kubernetes Namespaces or Cluster-Level Entities

Kubernetes documentation:

- Kubernetes API Concepts: Resource URIs
- Kubernetes API
- Extend the Kubernetes API with CustomResourceDefinitions

etcd Backup and Recovery

You can protect the etcd key value store and associated control plane SSL certificates, for complete protection of Kubernetes applications, API resources, and the cluster configuration. You can protect etcd in single-node, multi-node, and stacked high-availability (HA) cluster configurations. Commvault uses etcd built-in snapshots to capture the etcd data.

From the kubernetes.io documentation:

- *etcd is a consistent and highly-available key value store used as Kubernetes' backing store for all cluster data.*
- *All Kubernetes objects are stored on etcd. Periodically backing up the etcd cluster data is important to recover Kubernetes clusters under disaster scenarios, such as losing all control plane nodes.*

Key Features

- Back up etcd using built-in snapshots
- Back up etcd SSL certificates that are associated with Kubernetes control-plane nodes
- Recover from disaster scenarios of a single control plane node or a loss of all control plane nodes

Applicable Agents

Virtual Server Agent for Kubernetes

Setup Requirements

Enable the **etcd protection** setting for the cluster.

More Information

Commvault documentation:

- Enabling Kubernetes etcd key-value store Backups
- Configuring Protection for etcd SSL Certificates
- Backing Up etcd On Demand for Kubernetes
- Restoring a Kubernetes etcd Snapshot to a File System

Kubernetes documentation:

- etcd.io
- Operating etcd clusters for Kubernetes
- Stacked etcd topology

Complete: Protect Virtual Environments

Back Up and Restore Instances That Are Under Sub-Compartments for OCI Regions

You can back up and restore instances that are under sub-compartments (up to six levels deep) for OCI tenancy.

More Information

- Backups for Oracle Cloud Infrastructure
- Restoring Full Instances for Oracle Cloud Infrastructure

Encrypt Azure VMs Using a Different DES Than Its Source

You can restore existing Azure VMs or convert other hypervisor VMs to Azure using a different disk encryption set (DES) than their source.

To encrypt a VM with a different DES, you must select the relevant encryption type and set during out of place restores.

More Information

- Restoring Full Virtual Machines for Azure
- Converting to Azure Resource Manager
- Options for Conversion to Azure

Support for Azure-Managed VMs with Locked Azure Resources

Locked Azure resource groups can prevent the creation and deletion of snapshots during backup.

To enable backups and restores for a VM in a locked resource group, select an alternative, unlocked resource group in the VM group settings.

More Information

- Considerations for Locked Azure Resources
- Editing VM Group Settings for Azure

Enhancements to File Indexing for Virtual Machines

The following enhancements were made for file indexing for virtual machines:

- Using the Command Center, you can file index virtual machines using Indexing Version 2 for the following hypervisors:
  - Alibaba Cloud streaming backup
  - Google Cloud Platform streaming backup
  - Oracle Cloud Infrastructure streaming backup
  - vCloud Director streaming backup
- A Linux proxy can now be used to file index a virtual machine if the virtual machine has a basic disk and an NTFS file system (applicable for File Indexing Version 1 and File Indexing Version 2).

More Information

- File Indexing Version 2
- Requirements for File Indexing Version 1
- Requirements for File Indexing Version 2

Increased Hypervisor Support for Indexing V2

Indexing Version 2 is enabled for the following hypervisors:

- Citrix Xen
- Huawei FusionComplete
- OpenStack
- Oracle VM
- Oracle Linux Virtualization Manager
- Red Hat Virtualization

Indexing V2 provides VM-centric operations for virtualized workloads, such as granular backup, recovery, and control for individual VMs. Backup, restore and data aging, and security controls can be

controlled at an individual VM-level. When data for an individual VM needs specialized handling (for example, responding to a ransomware event), Indexing V2 allows fine-grained controls.

Starting with Commvault Platform Release 2022E, new hypervisors use Indexing V2 by default.

Key Features

- Perform backup, restore and data activity control at a single VM level.
- Replicate single VMs from streaming or IntelliSnap backups.
- Perform application-aware backups for individual VMs.

Applicable Agents

Virtual Server Agent (VSA) for:

- Citrix Hypervisor (XenServer)
- Huawei Fusion Compute
- OpenStack
- Oracle VM
- Oracle Linux Virtualization Manager
- Red Hat Virtualization

Setup Requirements

1. Upgrade the CommServe computer to CPR 2022E.
2. Download and run the Upgrade to Indexing V2 workflow to upgrade existing hypervisors to Indexing V2.

More Information

- Agents that Use Indexing (Indexing Version 1 and Indexing Version 2)
- Hypervisor Support for Indexing Version 2
- Commvault Store - Upgrade to Indexing V2 Workflow
- VM-Centric Operations in Command Center

Use Changed Block Tracking for Microsoft Azure Disk Encryption

You can now use changed block tracking (CBT) on Azure ADE encrypted VMs.

CBT enhances the backup performance of Azure virtual disks by comparing the changed blocks between Azure virtual disks snapshots. With this comparison, CBT for Azure provides better backup performance than traditional cyclic redundancy check (CRC) backups.

CBT is enabled by default and is applied to incremental backup and backup copy job types. It is available within Commvault Command Center and from the CommCell Console.

More Information

- Changed Block Tracking for Microsoft Azure

Disaster Recovery

Replicate AWS Instances to Azure Destination Sites

Replicate AWS instances to Azure destinations using replication groups. Use the Replication Monitor to track replication, failover, and failback operations.

More Information

- Creating a Replication Group Using the Replication Configuration Tool

Warm Site Recovery for Replication Groups

A warm site recovery replicates a source VM without creating a destination VM and disks on the disaster recovery (DR) site. You can also convert an existing replication group to a warm site to create the disaster recovery VM only during failover for non-critical VMs.

More Information

- Warm Site Recovery for Replication Groups

Replicate Azure Stack Hub VMs to Azure Destination Sites

Replicate Azure Stack Hub VMs to Azure destinations using replication groups. Use the Replication Monitor to track replication, failover, and failback operations.

More Information

- Creating a Replication Group Using the Replication Configuration Tool

Disaster Recovery for VMware VMs Using EBS Direct APIs

Commvault Disaster Recovery now leverages Amazon Elastic Block Store (Amazon EBS) direct APIs to

perform VMware to Amazon EC2 periodic replication. Amazon EBS direct APIs allow the creation of EBS snapshots directly, removing the need to create and attach volumes to the cloud access node in the destination region.

EBS direct API-powered periodic replication enables full instance VMware to Amazon EC2 restores within the same region, across regions, and across accounts.

Key Features

- Performs cross-vendor disaster recovery for VMware VMs to Amazon EC2 instances, using Amazon EBS direct APIs for data transfer.
- Accelerates replication of critical VMware VMs using cloud-native, API-driven data transfer methods.
- Reduces the cost and complexity of performing in-region and cross-region cross-vendor disaster recovery.

Applicable Agents

- Virtual Server Agent for VMware
- Virtual Server Agent for AWS

More Information

Commvault documentation:

- Periodic VM Replication Using Amazon EBS Direct APIs
- Installing Drivers Manually for HotAdd Replication from VMware
- Replication Group Options for Amazon
- Cross-Platform Feature Support for Replication

Amazon Web Services documentation:

- Amazon EBS direct APIs now enable you to create snapshots directly from any block storage
- Use EBS direct APIs to access the contents of an EBS snapshot

Journey To The Cloud

Linux CommServe Server

You can deploy a CommServe server in a Linux environment.

More Information

- CommServe Server in a Linux Environment - Getting Started

Restore AWS RDS Snapshots to a Different Cloud Account

You can restore an Amazon RDS instance to a different AWS cloud account. Previously, you could only restore an instance to the same account.

More Information

- Restoring an Amazon RDS Instance to the Same or a Different AWS Cloud Account

Convert an Azure Resource Manager Virtual Machine to a Google Cloud Platform Instance

When you restore an Azure Resource Manager virtual machine from a backup, you can restore it as a Google Cloud Platform (GCP) instance.

More Information

- Converting to Google Cloud Platform

Enable Cross-Region Copy of an Amazon Redshift Snapshot

You can enable and manage cross-region snapshot copies for Amazon Redshift snapshots.

More Information

- Enabling Cross-Region Copy of an Amazon Redshift Snapshot

Configuring an Access Node to Communicate with the Key Management Server

IAM role-based authentication for AWS and Managed Identity authentication for Azure is now supported to authenticate AWS or Azure Key Management Server (KMS) for third party key management. When you use these stronger authentication methods, you must designate an access node (MediaAgent) in cloud with the designated cloud roles to allow Commvault to properly authenticate to the KMS. You can also use access nodes to communicate to a third-party cloud KMS when the CommServe server does not or cannot have direct access to the KMS.

More Information

- Managing a Key Management Server

Clone Oracle and Oracle RAC PDBs in the Command Center

You can create a clone of an Oracle or Oracle RAC pluggable database (PDB), without a production database interruption. You can quickly create copies of your production data that is made up of Oracle PDBs.

Applicable Agents

- Oracle
- Oracle RAC

Setup Requirements

- A user-provided staging location is needed. The staging location must have enough free space for the datafiles for both the CDB and the PDB$SEED that you want to restore.
- The destination path must have enough free space for the PDBs that you clone.

More Information

- Cloning an Oracle PDB
- Cloning an Oracle RAC PDB

Azure Government Cloud Supported by Metallic Cloud Storage

Metallic Cloud Storage can be configured in government agencies using Azure Government Cloud. The Metallic Cloud Storage service offers a secure hybrid cloud strategy, which can be easily scaled out based on storage needs, without the need for additional infrastructure or cloud expertise.

Key Features

- Easy to implement because it is fully integrated with Commvault's Backup and Recovery software
- Easy to protect with built-in ransomware protection and optimizations for daily backups, typical retentions, and ad-hoc recoveries
- Easy to configure and manage using the unified Commvault Command Center interface, without the need to train or hire new personnel
- Predictable costs with no hidden fees for ingress or egress limits

More Information

- Metallic Cloud Storage
- Prerequisites For Metallic Cloud Storage

Run Startup Scripts on Google Cloud Platform Instances Using Custom Metadata

You can run startup scripts on restored or converted Google Cloud Platform instances using custom metadata.

To enable startup scripts on Google Cloud Platform, configure the Custom metadata settings during out of place restores.

More Information

- Converting to Google Cloud Platform
- Options for Conversion to Google Cloud Platform
- Restoring Full Instances for Google Cloud Platform

Associate Nodes or Node Groups with a Restored Google Cloud Platform Instance

While performing a full, out-of-place restore for Google Cloud Platform, you can select the nodes or node groups you want to associate with the restored instance.

More Information

- Restoring Full Instances for Google Cloud Platform
- Converting to Google Cloud Platform
- Options for Conversion to Google Cloud Platform

Convert Virtual Machines from Hyper-V to Amazon Web Services

In the Command Center, when you restore a Hyper-V backup, you can convert it to an Amazon EC2 instance.

More Information

- Converting to AWS

Hardware Security Module (HSM) for Google Cloud Platform

You can use HSM protection with a customer-managed encryption key for streaming backups, IntelliSnap backups, and backup copies of Google Cloud Platform.

More Information

- Backups for Google Cloud Platform

Convert and Replicate Additional Guest OSes to AWS Destinations

Commvault has expanded the list of guest OSes that you can convert from VMware, Azure, and Hyper-V to AWS. The list of guest OSes has also expanded for Disaster Recovery from VMware to AWS. You can securely migrate additional guest operating systems when you perform self-service, Commvault orchestrated migration, and Disaster Recovery from on-premises to Amazon EC2 instances.

Additional guest operating systems (and minor releases) include the following:

Linux/Unix (64-bit only)

- CentOS 8.0-8.2, 6.1-6.8
- Oracle Linux 8.0-8.6, 7.0-7.9, 6.0-6.10
- Red Hat Enterprise Linux (RHEL) 8.0-8.6
- Ubuntu 14.04, 14.10, 15.04, 16.10, 17.04, 18.04, 20.04, 21.10, 22.04
- SUSE Linux Enterprise Server 15 with Service Pack 1, Service Pack 2, Service Pack 3

Windows (64-bit only)

- Microsoft Windows Server 2019 (Standard, Datacenter)
- Microsoft Windows Server 1803 (Standard, Datacenter)
- Microsoft Windows Server 1709 (Standard, Datacenter)
- Microsoft Windows Server 2016 (Standard, Datacenter)
- Microsoft Windows Server 2012 R2 (Standard, Datacenter) (Nano Server installation not supported)
- Microsoft Windows Server 2012 (Standard, Datacenter)
- Microsoft Windows 10 (Home, Professional, Enterprise, Education) (US English)
- Microsoft Windows Server 2008 R2 (Standard, Web Server, Datacenter) (64-bit only)

Note:
For Windows pre-installation, Commvault no longer requires disabling of the Windows firewall, User Access Controls (UAC), AutoAdminLogin enabled, or AWS PVDriver.

Key Features

- Self-service VMware, Azure, and Hyper-V conversion and VMware replication to Amazon EC2 instances for a broader set of Windows and Linux releases.
- Simplified cross-vendor migration and Disaster Recovery through intelligent orchestration leveraging Amazon EBS direct APIs.
- Prescriptive guidance for ensuring successful Linux-based guest migration and Disaster Recovery.

Applicable Agents

VM Conversion (Cross-Hypervisor Restore):

- Virtual Server Agent for Azure to AWS
- Virtual Server Agent for Hyper-V to AWS
- Virtual Server Agent for VMware to AWS

Disaster Recovery Replication:

- Virtual Server Agent for VMware to AWS

More Information

- Cross-Hypervisor Restores (VM Conversion)
- Cross-Platform Feature Support for Replication
- VM Conversion Using Commvault HotAdd - Supported Guest Operating Systems
- VM Conversion Using EBS Direct APIs - Supported Guest Operating Systems
- Periodic VM Replication Using Amazon EBS Direct APIs - Requirements
- Periodic VM Replication Using Amazon EBS Direct APIs - Supported Guest Operating Systems
- Configuring Windows Source VMs for VM Conversion Using Commvault HotAdd - Procedure
- Installing Drivers Manually for EBS Direct API Replication from Amazon Web Services

Modern Infrastructures

Containerized Web Server

You can use the Commvault software to install and run a standalone Linux Web Server in a Kubernetes cluster.

Setup Requirements

Kubernetes
You can use Kubernetes 1.16 and later versions.
Docker
You can use Docker Engine 17.06 and more recent versions.
Base Image for Commvault Container
You can use the following versions of centOS for your base image:

- CentOS 7.9.2009
- CentOS 7.8.2003
- CentOS 7.7.1908
- CentOS 7.6.1810
- CentOS 7.5.1804
- CentOS 7.4.1708
- CentOS 7.3.1611
- CentOS 7.2.1511
- CentOS 7.1.1503
- CentOS 7.0.1406
- CentOS 7
- CentOS 6.10
- CentOS 6.9
- CentOS 6.8
- CentOS 6.7
- CentOS 6.6
- CentOS 5.11
- CentOS 5

More Information

- Containerized Web Server

Understand And Activate Data

Monitor Growth Trends for File Storage Optimization (FSO)

FSO now provides weekly/monthly storage growth trends to help storage administrators. You can use this information to do the following:

- Understand the historical rate of storage growth or contraction
- Fine-tune Information Lifecycle Management (ILM) / Data Retention policies

- Plan storage infrastructure requirements

More Information

- Information Available on the Trending Data Dashboard

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