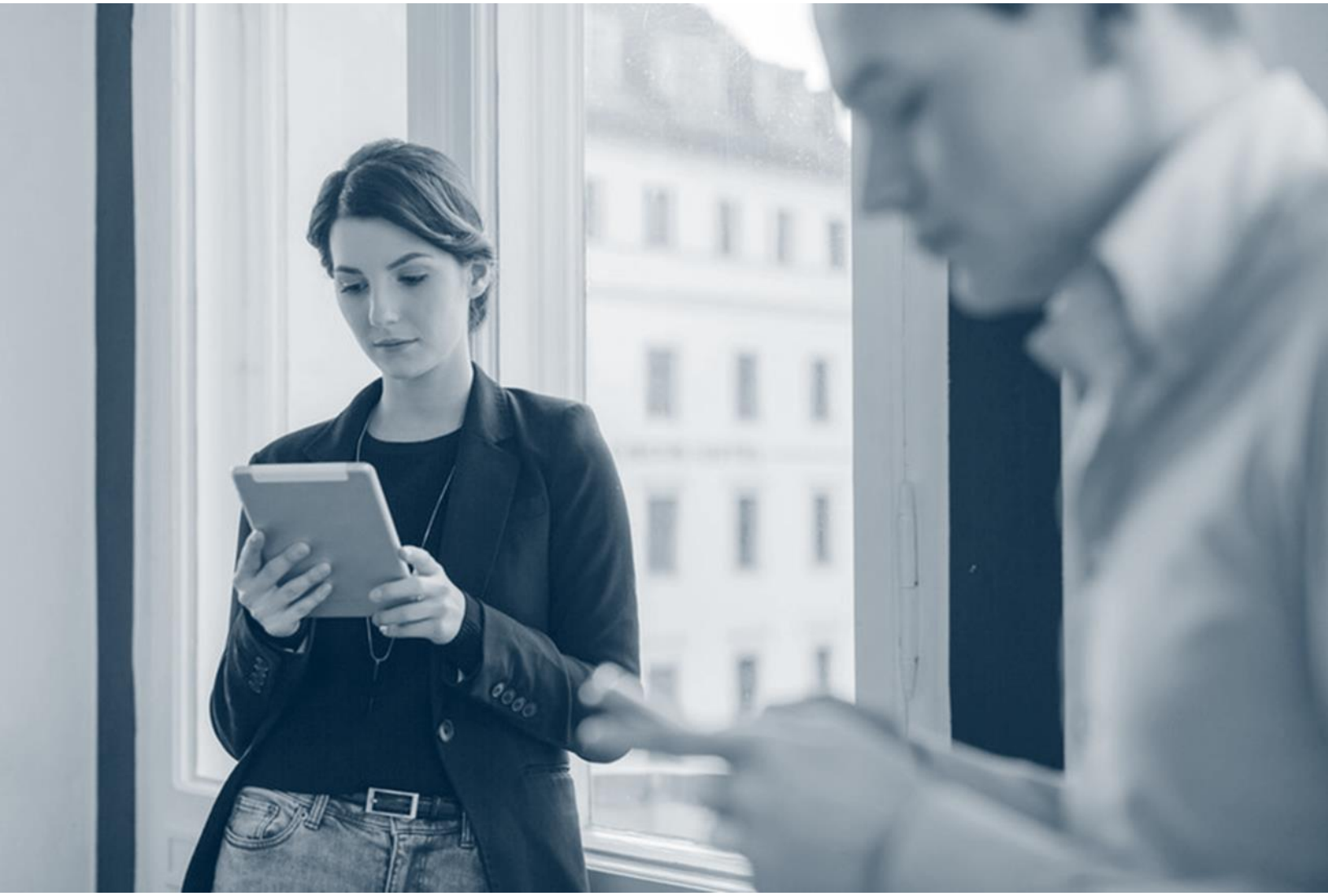
COMMVAULT

11.21 Newsletter

September 15, 2020



Contents

Complete Backup And Recovery 3

Back Up and Restore SAP HANA Databases with SSL Connections 3

Reduce the RPO to Minutes with Streamlined Log Backups Using Disk Caching for Informix Databases 3

IntelliSnap for Instances on Google Cloud Platform 3

Microsoft SharePoint Server Agent Supports Modern Authentication 4

Side-by-Side Installation of Maintenance Releases 4

Configure Commvault VTL for IBM i from the Command Center 5

Identify Crucial CommCell Settings Using the CommCell Configuration Audit Report 5

Back Up and Restore HCL Domino Version 11 6

View the DB2 Version Upgrade History 6

Complete: Manage New Workloads 7

Back Up and Restore MongoDB Sharded Clusters or Replica Sets in the Command Center 7

Seamless Restores of Copy-Only Full Backups for SQL Always-On Availability Groups 7

VSA Support for MEDITECH on Nutanix AHV 8

Complete: Protect Virtual Environments 8

Cross-Account Copying of Amazon Snapshots for RDS and EC2 8

Deploy Commvault to Protect Workloads Running in the Azure VMware Solution 9

For Azure Managed Disks, Back Up and Restore Azure Availability Zones Information 9

Journey To The Cloud 10

Back Up and Restore Nutanix Files in the Command Center 10

IntelliSnap for Google Cloud Platform 11

Cross-Account Data Management By Using Security Token Service (STS) AssumeRole API and 11

Authenticate Azure SQL Databases Using Managed Identities 12

Convert Virtual Machines from Hyper-V to Azure Stack Hub 13

Azure NetApp Files for SAP HANA 13

Back Up and Restore Regional Persistent Disks for Google Cloud Platform 14

Replicate SAP HANA Databases in Cloud 14

File System Restores to Cloud Storage Accounts 15

Incremental Snapshots for Applications in Azure Infrastructure with Managed Disks 15

Creating VM Disk Filters for Google Cloud Platform 15

Back Up and Restore Amazon EC2, RDS, and EKS Workloads, and MySQL and PostgreSQL 16

Automatically Scale Azure Access Nodes 17

Modern Infrastructures 17

Configure an Identity Provider CommCell to Manage Multiple CommCells 17

Enable a Passkey for Browsing and Restoring Backup Data 17

Configure Ransomware Protection for Disk Libraries on a Linux MediaAgent 18

Allow Override Restrictions for Retention Settings in Laptop Plans 19

Orchestration And Automation 19

Validate Backups of VMware Virtual Machines 19

Understand And Activate Data 20

Capture Additional Data for NetApp Data Sources in Activate 20

Analyze NFS Exports in File Storage Optimization 20

Complete Backup And Recovery

Back Up and Restore SAP HANA Databases with SSL Connections

You can back up and restore SAP HANA databases that use SSL (Secure Sockets Layer) connections.

More Information

- Enabling SSL Communication with the SAP HANA System

Reduce the RPO to Minutes with Streamlined Log Backups Using Disk Caching for Informix Databases

For Informix, you can run streamlined log backups on a schedule that supports backup frequencies as small as 5 minutes.

Streamlined log backups use caching to a disk library to reduce the backup time for database instances that have a high transaction rate. The backups are written to disk mount paths that are managed by the MediaAgent, so you do not need to store the backups on production servers. The database client and the MediaAgent run the log backups, independent of the CommServe server, which increases the availability of the database client and MediaAgent pair, while also reducing the load on the CommServe application. A second operation periodically commits and registers the logs, to support copy operations. Log backups continue even if the CommServe server is unavailable.

Applicable Agents

Informix agent

More Information

- Disk Caching for Frequent Log Backups
- Optimizing Informix Log Backups

IntelliSnap for Instances on Google Cloud Platform

You can use IntelliSnap to back up and recover instances that are hosted in Google Cloud Platform. Configure IntelliSnap backup and restore operations from the Command Center.

Applicable Agents

Virtual Server Agent

More Information

- IntelliSnap Support for Virtualization

Microsoft SharePoint Server Agent Supports Modern Authentication

Microsoft is deprecating basic authentication in October 2020. SharePoint Server Agent now supports both basic and modern authentication.

Key Features

With this feature, Office 365 SharePoint solutions can use modern authentication to protect SharePoint online data.

More Information

- SharePoint Online
- Microsoft Office 365 with SharePoint Server

Side-by-Side Installation of Maintenance Releases

You can install maintenance releases side-by-side as follows:

- The latest maintenance release will be installed on the CommServe computer using the software that is currently in the cache. If there is nothing in the cache, the system will automatically download the latest available maintenance release and then push it to the CommServe computer.
- For a client whose current feature release is older than the feature release that is installed on the CommServe computer, the maintenance release that is available in the cache for the client's current feature release will be installed on the client. If there is nothing in the cache, you must first download the maintenance release.
- For a client whose current feature release is the same as the CommServe computer's feature release, the maintenance release that is currently in the cache will be installed. If there is nothing in the cache, the system will automatically download the maintenance release that is installed on CommServe computer, and then push it to the clients.
- You can push to a client a maintenance release that is higher than the maintenance release that is installed on the CommServe computer. To do this, you must first download the maintenance release to the cache.

More Information

- Download and Sync Cache Options (General)
- Cache Details
- Software Cache Configuration (CommServe Software Cache)
- Software Cache Configuration (Remote Software Cache)
- Update Software

Configure Commvault VTL for IBM i from the Command Center

You can configure a Commvault Virtual Tape Library (VTL) for IBM i from the Command Center to back up and restore IBM i data.

Key Features

- Commvault VTL improves backup-restore throughput by going over a fibre channel.
- Commvault VTL simplifies disaster recovery of IBM i servers.

Applicable Agents

IBM i File System Agent

Setup Requirements

- Install Commvault VTL for the IBM i File System Agent on the Linux access node.
- Configure Fibre Channel (FC) network zoning to allow access to the Linux access node FC target from the IBM i server.

More Information

- Installing VTL on the Linux Access Node

Identify Crucial CommCell Settings Using the CommCell Configuration Audit Report

For optimal CommCell performance, configure the settings in your CommCell environment to match the recommended Commvault settings that are identified in the CommCell Configuration Audit report.

Key Features

The following settings are compared in this report:

- Disk and tape library settings
- Storage policy and storage policy copy settings
- Media management settings
- Data aging settings

Setup Requirements

Private Metrics Reporting Server

More Information

- CommCell Configuration Audit Report

Back Up and Restore HCL Domino Version 11

You can back up and restore HCL Domino Version 11 data.

Key Features

The way that you perform backups and restores for Domino Version 11 is the same as for previous versions of Domino.

More Information

- Notes Database Agent: System Requirements
- Notes Document Agent: System Requirements
- Domino Mailbox Archiver Agent: System Requirements

View the DB2 Version Upgrade History

You can view the DB2 version upgrade history in the Command Center or CommCell Console.

Applicable Agents

DB2 agent

More Information

- View the DB2 version upgrade history in the Command Center
- View the DB2 version upgrade history in the CommCell Console

Complete: Manage New Workloads

Back Up and Restore MongoDB Sharded Clusters or Replica Sets in the Command Center

You can back up and restore MongoDB sharded clusters or replica sets in the Command Center.

You can restore the MongoDB data to the same or a different replica set or to a sharded cluster that has the same number of shards as the source cluster.

Key Features

- Uses Commvault IntelliSnap technology to protect the cluster
- Protects both replica set topologies and sharded cluster topologies
- Protects the MongoDB databases from the secondary node, without using the primary node resources
- Allows recovery of the entire cluster
- Allows recovery to the original cluster or to a different cluster with the same number of shards, on-premises or within the cloud

More Information

- MongoDB

Seamless Restores of Copy-Only Full Backups for SQL Always-On Availability Groups

You can configure SQL Availability Group instances to run full backups as copy-only full backups on the secondary replica in an Always-On configuration instead of running the full backup on the primary replica.
The SQL agent automatically chains any subsequent log backups to the copy-only full backup, which enables seamless recovery from copy-only full backups.

More Information

- Configuring Copy-Only Backups on Availability Group Instances

VSA Support for MEDITECH on Nutanix AHV

You can use the Commvault software through the Command Center to back up your MEDITECH file server VMs that are hosted in a Nutanix Acropolis Hypervisor (AHV) cluster.

From the Command Center, you can:

- Back up MEDITECH VMs
- Restore full MEDITECH VMs (in place and out-of-place)

Applicable Agents

Virtual Server Agent

More Information

- MEDITECH with Nutanix AHV for the Command Center

Complete: Protect Virtual Environments

Cross-Account Copying of Amazon Snapshots for RDS and EC2

You can replicate and create Amazon RDS and EC2 full copy snapshots to a different Amazon account in the same or in a different geographic region for your disaster recovery needs. Copying snapshots to a different account prevents snapshot corruption and accidental deletion.

Key Features

- You can restore data from the copied snapshot even if the source snapshot or the source RDS or EC2 instance is deleted, thereby providing an additional layer of security or air gap.

Applicable Agents

- Amazon RDS
- VSA for Amazon

Setup Requirements

The source Amazon account can be configured with an access key and secret key, an IAM role, or an STS role ARN. The destination Amazon account must be configured with an access key and secret key or an STS role ARN.

More Information

- Creating a Snapshot Copy of Amazon RDS or an Aurora Database in a Different Account
- Creating a Snapshot Copy of Amazon EC2 in a Different Account

Deploy Commvault to Protect Workloads Running in the Azure VMware Solution

You can deploy Commvault to protect workloads running in the Azure VMware Solution (AVS).

Key Features

With AVS, you can perform the following:

- Backups and restores using vStorage APIs for Data Protection (VADP)
- Changed block tracking (CBT)
- Full, incremental, differential, and synthetic full backups
- Restores of full VMs, VMDKs (alone or attaching to a VM), and guest files and folders
- Agentless file recovery
- Application-aware backups
- VM conversion from VMware to Microsoft Azure
- VM conversion from Microsoft Azure to VMware
- Live Sync replication and Live Sync Direct for snapshot-based replication
- Replication from VMware to Microsoft Azure

Applicable Agents

Virtual Server Agent for VMware

More Information

- Support for Azure VMware Solution

For Azure Managed Disks, Back Up and Restore Azure Availability Zones Information

For Azure managed disks, you can back up and restore virtual machines that contain information

regarding the Azure Availability Zones. Azure Availability Zones are configured specific locations (physical) within an Azure region.

Azure Availability Zones information is included in streaming backups, IntelliSnap backups, and backup copies. When you restore Azure virtual machines, if the region to which you are restoring your VM supports Azure Availablity Zones, then the Availability Zones information will be restored to the destination VM.

You can run backups and restores for Azure managed disks from the Command Center and the CommCell Console.

Applicable Agents

Virtual Server Agent for Azure

More Information

- Backups for Azure (Command Center)
- Backups (CommCell Console)

Journey To The Cloud

Back Up and Restore Nutanix Files in the Command Center

You can back up and restore data (CIFS shares and NFS exports) that resides on your Nutanix Files file server in the Command Center.

Key Features

You can use the Command Center to perform the following tasks:

- Quickly configure file servers, storage, and subclients to back up
- Back up subclients immediately or on a schedule
- Restore CIFS shares and NFS exports to the source Nutanix Files file server or any other file location
- Monitor jobs, events, and alerts

Applicable Agents

- Windows File System Agent
- Linux File System Agent

More Information

- Nutanix Files

IntelliSnap for Google Cloud Platform

You can use IntelliSnap to take snapshots of data on Google Cloud platform.

The snapshots are used for in-place and cross-server recovery, as well as for creating clones of databases to another server in the cloud.

Applicable Agents

- Oracle
- SAP HANA
- UNIX File System
- Windows File System

More Information

- Google Cloud Platform

Cross-Account Data Management By Using Security Token Service (STS) AssumeRole API and Amazon IAM Roles

Use STS AssumeRole capability in the backup and management of Amazon EC2, EBS, EKS, IAM, KMS, RDS, S3, and SSM services.

Amazon Identity and Access Management (IAM) provides a method for end-users to replace the user name and secrets based authentication with IAM Roles. Amazon STS AssumeRole capability extends IAM Roles by allowing one Amazon user to request temporary credentials of another user.

Key Features

- Use STS:AssumeRole to centralize backup operations, while assuming the role of each protected sub-account during backup activities.
- Remove the requirement to provision Amazon Access Nodes per account, by using a single pool of Access Nodes to protect many accounts.
- Remove the use of Access Key/Secret Key configurations which require manual key rotation to stay secure over time.

Applicable Agents

- Virtual Server Agent (VSA) for Amazon
- Virtual Server Agent for Elastic Kubernetes Service (EKS)
- Cloud Apps agent for Amazon S3

Setup Requirements

- At least two distinct Amazon accounts or IAM Roles must exist.
- The sub-account must explicitly trust the organizational service account to permit request of temporary credentials from the STS service.
- Both the service account and the sub-account must have the permissions to perform backup via either amazon_permission_backup_restore.json or amazon_restricted_role_permissions.json.
- The service account must be granted permission to call the STS:AssumeRole() API call.
- The Amazon Access Node must have layer 3 connectivity to https://sts.amazonaws.com either directly or via HTTP PROXY.

More Information

- Configuring STS Role Authentication
- Creating a Role with Restricted Access
- Creating a vmimport role
- Amazon Web Services Permission Usage
- Guided Setup for Amazon
- Adding an Amazon Hypervisor
- Creating an Amazon RDS Client
- Enabling Cross-Account Sharing of an Amazon RDS Snapshot Copy
- Using an IAM Role to Grant Permissions to Applications Running on Amazon EC2 Instances
- AWS Security Token Service
- AssumeRole

Authenticate Azure SQL Databases Using Managed Identities

You can now authenticate Azure SQL database backup and restore operations using Azure Managed Identities.

Managed identities is a secure authentication method for Azure cloud services that allows only authorized managed-identity-enabled virtual machines to access your Azure subscription.

Key Features

Provides Azure services with an automatically managed identity in Azure AD. You can use the identity to authenticate any service that supports Azure AD authentication without the need to store the credentials in the source code.

Applicable Agents

Azure SQL Server database

Setup Requirements

- The user must have Service Administrator role privileges.
- The access nodes must be in the Azure cloud.

More Information

- Configuring an Azure SQL Instance

Convert Virtual Machines from Hyper-V to Azure Stack Hub

When restoring a virtual machine from a backup for Hyper-V, you can convert the VM to Azure Stack Hub.

This feature can be used to migrate workloads to Azure Stack Hub, and is available in the Command Center.

Applicable Agents

Virtual Server Agent

More Information

- Converting to Azure Stack Hub

Azure NetApp Files for SAP HANA

You can use the IntelliSnap capability to take snapshots of SAP HANA databases with Azure NetApp Files.

Applicable Agents

SAP HANA

More Information

- Azure NetApp Files for SAP HANA

Back Up and Restore Regional Persistent Disks for Google Cloud Platform

For Google Cloud Platform (GCP), you can back up and restore regional persistent disks (standard and solid-state drive).

When regional persistent disks reside on an instance that is configured for backups and restores, the regional persistent disks are included in the backups. You can then restore the instance that includes these disks either in-place or to a new destination.

For out-of-place restores, if the instance that you are restoring includes regional disks, all the regional disks are restored to the selected zone.

You can configure GCP backup and restore operations from the Command Center.

More Information

- Backups for Google Cloud Platform

Replicate SAP HANA Databases in Cloud

Use Live Sync to replicate SAP HANA databases running on cloud infrastructure like Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP).

The Live Sync operation integrates with cloud native snapshots and replicates the incremental changes of a database to a synced copy of the database. The replication is triggered automatically when an IntelliSnap backup runs on the source database.

More Information

- Replication of SAP HANA Databases

File System Restores to Cloud Storage Accounts

From the Command Center, you can restore backed-up data to the following cloud storage accounts:

- Alibaba Cloud
- Amazon S3
- Azure Blob Storage
- Azure Data Lake Storage Gen2
- Azure File Storage
- Google Cloud
- IBM Cloud Object Storage (COS)

Applicable Agents

File System Agent

More Information

- Performing File System Restores to Cloud Storage Accounts

Incremental Snapshots for Applications in Azure Infrastructure with Managed Disks

IntelliSnap for Azure Managed Disks includes the following enhancements:

- Create incremental snapshots for Azure managed disks, by default. Incremental snapshots are cost effective point-in-time backups that store only the changes on the disks since the most recent snapshot.
- Optimize the snap operation performance by reducing the time taken to mount and unmount from multiple Azure disks.

More Information

- Microsoft Azure Snap

Creating VM Disk Filters for Google Cloud Platform

You can manage your VM group content by creating disk filters to exclude virtual machine disks from backups.

You can create disk filters in the Command Center.

More Information

- Creating Disk Filters for Google Cloud Platform

Back Up and Restore Amazon EC2, RDS, and EKS Workloads, and MySQL and PostgreSQL Databases, on AWS Outposts

You can back up and restore EC2, RDS, and EKS workloads, and MySQL and PostgreSQL databases, running in Amazon Web Services (AWS) Outposts.

Also, you can replicate and migrate workloads between the AWS region and Outposts.
AWS Outposts is an on-premises, fully-managed deployment of AWS EC2, RDS, and EKS services, infrastructure, and operations that provides hybrid cloud capabilities.

Key Features

- Back up and recover AWS Outposts-hosted workloads.
- Cloud native snapshot orchestration and back up to Commvault cloud libraries.
- Ensure data residency needs are met for AWS Outposts backup data with plans.
- Migrate data between AWS region and AWS Outposts with Commvault automation.
- Extend your Disaster Recovery landscape with failover/failback between AWS region and AWS Outposts, and vice versa.

Applicable Agents

- Virtual Server Agent (VSA) for Amazon.
- Virtual Server Agent (VSA) for Amazon Web Services (EC2, RDS, EKS).
- MySQL Agent (if performing MySQL dump/export backup)
- PostgreSQL Agent (if performing PostgreSQL dump/export backup).

Setup Requirements

- At least one AWS access node is required to perform EC2, RDS, and EKS backups.
- The access node for EC2 and RDS backups must be located in the AWS region.
- The access node for EKS and RDS dump/export backups must be located within AWS Outposts.
- AWS Outposts workloads are identified by subnet only. Commvault recommends the use of AWS tagging to identify AWS Outposts applications for backup and restores.
- AWS Outposts does not currently provide Amazon S3 storage. All EBS snapshots are stored in the region.
    - If localized backup copies are required (within AWS Outposts), the EBS volumes can be provisioned as a Commvault disk library.
    - Commvault can be directed to write to local storage devices outside your AWS Outposts via an Amazon Local Gateway (LGW).

More Information

- AWS Outposts

Automatically Scale Azure Access Nodes

You can use the automatic scaling feature to launch access nodes in Azure only when you need to back up VMs, and then decommission the access nodes soon after you use them. This feature reduces the amount of time that you use Azure access nodes for backup, and can also reduce the cost of using them.

Key Features

- Automatically creates up to 100 access nodes to back up VMs.
- Automatically decommissions access nodes after 1 hour of inactivity using the Power Management feature and the Lifecycle Management feature.

More Information

- Automatic Scaling for Azure Access Nodes

Modern Infrastructures

Configure an Identity Provider CommCell to Manage Multiple CommCells

In a CommCell environment, you can configure a CommCell to act as the Identity Provider (IdP) CommCell to manage other CommCells that you add as service CommCells. The user can log on to the Command Center of the IdP CommCell, and then access and manage the service CommCells.

More Information

- Managing Service CommCells

Enable a Passkey for Browsing and Restoring Backup Data

When you create and require a passkey for a client computer, end-users must enter the passkey whenever they attempt to browse and restore backup data on the client computer. This ensures that

only authorized users have access to client computer backup data.

In a CommCell environment, MSP administrators can create and require a passkey for all client computers at the CommCell and company levels. Similarly, tenant administrators can create and require a passkey for all their client computers at the company level.

In addition, the MSP administrator and tenant administrators can enable the passkey feature for client owners, so that client owners can create and require a passkey for each of their client computers.

Key Features

- After enabling a passkey, the **Authorize for restore** option appears. Enable the **Authorize for restore** option to allow an end-user that entered the correct passkey to browse and restore backup data for a period of thirty minutes.
- An MSP administrator and tenant administrator can enable and require the passkey feature, using the Command Center.
- A client owner can create and require the passkey feature using the Command Center, Web Console, and CommCell Console.
- All users (the MSP administrator, tenant administrators, and client owners) can use REST API requests to create and require a passkey for a client computer.
- If passkeys are defined at multiple levels, the lowest level passkey takes precedence. For example, a passkey that is configured for a client computer takes precedence over a passkey that is configured for a company, and a user who is performing a restore for the client computer must use the passkey that is configured by the client owner.

More Information

- Requiring a Passkey as an MSP Administrator
- Enabling CommCell environment Client Owners to Require a Passkey
- Configuring a Passkey in the Command Center as a Tenant Administrator
- Configuring a Passkey in the CommCell Console as a Tenant Administrator
- Enabling Company Client Owners to Require a Passkey
- Requiring a Passkey in the Command Center as a Laptop Device Owner
- Configuring a Passkey in the Commcell Console as a Client Owner
- Configuring a Passkey as a Client Owner in the Web Console
- Creating a Passkey for Virtual Machine Restores
- REST API - POST Passkey (Company Level)
- REST API - POST Authorize for Restore (Company Level)
- REST API - POST Passkey (Client Level)
- REST API - POST Authorize for Restore (Client level)

Configure Ransomware Protection for Disk Libraries on a Linux MediaAgent

You can configure ransomware protection for local and mounted disk libraries on a Linux MediaAgent

and on a node in a HyperScale storage pool. After you configure ransomware protection, only certain white-listed Commvault processes can modify the backup data that is present on the MediaAgent. This protection greatly reduces the risk of a ransomware attack on the backup data.

More Information

- Ransomware Protection for Disk Libraries on a Linux MediaAgent

Allow Override Restrictions for Retention Settings in Laptop Plans

You can set override restrictions in laptop base plans. Plans that are derived from base plans can inherit or modify the retention settings that are specified in the base plans.

More Information

- Creating a Laptop Plan

Orchestration And Automation

Validate Backups of VMware Virtual Machines

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

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

You can configure validation for a VM group in the Command Center, and monitor validation from the Virtualization dashboard.

Applicable Agents

Virtual Server Agent

Setup Requirements

- To specify a standard location where VMs are mounted, or to enable non-admin users to configure backup validation, create a recovery target.
- Create a VM group for each set of guest VMs that run an application. For example, you can create one VM group for VMs that run SQL Server, and a separate VM group for VMs that run Exchange.
- Obtain credentials for guest VMs that run applications.
- Use a Windows access node (VSA proxy) for application validation.
- If necessary, create custom validation scripts for applications. A script for SQL Server is included with the Virtual Server Agent package.

More Information

- Application Validation for VMware VMs

Understand And Activate Data

Capture Additional Data for NetApp Data Sources in Activate

File monitoring tracks file activities such as who accessed, modified, deleted, or renamed a file, and provides the information required to remediate files. For example, you can determine the exposure of a sensitive document by reviewing the number of users who accessed the document. File monitoring information is available in Sensitive Data Governance and File Storage Optimization for files residing on a NetApp file server.

More Information

- Viewing File Monitoring Information
- Adding File System Data Sources to a Project

Analyze NFS Exports in File Storage Optimization

In File Storage Optimization, you can analyze data in an NFS export even if a file system agent is not installed.

More Information

- Adding a File Server Data Source for File Storage Optimization

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