

IBM® Storage

Cyber Resilience Solution Across Hybrid Cloud Using IBM Storage Solutions

IBM

© Copyright International Business Machines Corporation 2020.

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

About this document	1
Executive summary	1
Scope	1
Prerequisites	2
National Institute of Standards and Technology framework	2
Implementing Hybrid Cloud Cyber Resilience Solution with IBM Spectrum Protect Plus and IBM Cloud Object Storage	3
IBM FlashSystem	4
IBM Spectrum Protect Plus	4
IBM Cloud Object Storage	4
IBM Cloud	4
Establish site-to-site IPSec VPN for hybrid-cloud connectivity with IBM Cloud	5
Architectural overview of Hybrid Cloud Cyber Resilience solution	6
Considerations	7
Setting up Hybrid Cloud Cyber Resilience solution	8
On-premises setup and configuration	8
IBM Cloud setup and configuration	9
VMware vSphere ESXi server setup in IBM Cloud	9
IBM Cloud Object Storage configuration in IBM Spectrum Protect Plus	16
Creating a Cyber Resilience SLA policy in IBM Spectrum Protect Plus	18
Cyber Resilience Solution use cases	20
Protecting virtual machine data to IBM Cloud Object Storage WORM buckets	21
Copying protected data from remote vSnap server to IBM Cloud Object Storage WORM buckets	23
Recovering data from IBM Cloud Object Storage	24
Restoring virtual machines to the primary site	27
SQL Server data backup to IBM Cloud Object Storage WORM buckets	30
Recovering SQL Server data from IBM Cloud Object Storage	32
Backing up and recovering the IBM Spectrum Protect Plus server	34
Conclusion	35
Related resources	35
About the author	36
Acknowledgments	36
Notices	39
Trademarks	40
Terms and conditions for product documentation	41
Applicability	41
Commercial use	41
Rights	41
Privacy policy considerations	41



About this document

This document is intended to facilitate the deployment of the Hybrid Cloud Cyber Resilience solution for storage system data that it backed up in IBM Spectrum Protect Plus from external cyberattacks or insider attacks by using its integration with IBM Cloud Object Storage. You must understand IBM FlashSystem, IBM Spectrum Protect Plus, and IBM Cloud Object Storage architecture concepts and its configuration across hybrid cloud.

The information in this document is distributed on an as-is basis without any warranty that is either expressed or implied. Support assistance for the use of this material is limited to situations where IBM FlashSystem, IBM Spectrum Protect Plus or IBM Cloud Object Storage are supported and entitled, and where the issues are specific to a solution technical paper implementation.

Executive summary

In today's data driven world, the information and data of an organization is considered as the most important asset to its business. It can serve as key asset for growth of an organization. As more data are collected by organizations, it is growing at a staggering pace. With this exponential data growth, there is an increase need to protect the data from the various cyberattacks in the form of malware and ransomware that is trying to steal precious data and information. These cyberattacks can have catastrophic impact on the organization and result in devastating financial losses and affect the organization's reputation for years.

Scope

This solution technical paper provides the following information:

- A solutions architecture and related solution configuration workflows, with the following essential software components:
 - IBM FlashSystem or any IBM Spectrum Protect Plus supported storage system
 - IBM Spectrum Protect Plus
 - IBM Cloud Object Storage configuration inside IBM Cloud
- Detailed technical configuration steps for building an end-to-end solution

This technical report does not make the following changes:

- Provide scalability and performance analysis from a user perspective
- Provide claims of creating isolated air-gap infrastructure
- Replace any official manuals and documents that were issued by IBM

Prerequisites

This technical paper assumes basic knowledge of the following prerequisites:

- IBM FlashSystem (or IBM Spectrum Protect Plus supported storage system) installation and configuration
- IBM Spectrum Protect installation and configuration
- IBM Cloud Object Storage installation and configuration
- VPN connectivity between on-premises network and IBM Cloud network
- VMware vSphere installation and configuration

National Institute of Standards and Technology framework

As systems became linked with external networks, organizations adopted a “defense-in-depth” security mode so that if the perimeter was breached, more layers of security were available to protect critical information from falling into the wrong hands. The focus was on the technical aspects of recovery. However, these measures are no longer sufficient for the protection against cyberattacks.

Organizations are understanding that traditional device and technology-centric security measures, such as firewalls, fail to provide security in the cyber ecosystem. As we move forward, we must take a holistic approach across our data, applications, and the entire infrastructure to not only recover, but prevent or at least minimize the attack.

Some of the following factors are considered for designing Cyber Resilience approach:

- While regulations continue to play an important role, consumers decide the ultimate outcomes for a business.
- For implementing effective Cyber Resilience approach, it must be changed from reactive approach to the proactive approach. A repeated cycle of planning, protecting, testing, and learning must be implemented by a Cyber Resilience team.
- Most organization’s backup and disaster recovery plans are designed around the fact that most disasters are caused by technical failures or human errors with a secondary concern of natural disasters. Modern data protection approaches should also consider the data compromise factor because of cyber events and be implemented accordingly.
- Because attackers are getting smarter, approaches must consider continuous improvements, innovations, and reengineering to address the newer threats that are challenging the organizations.
- Although the effort is to use existing infrastructure, modern technologies help automate the systems to deal more effectively with the cyberthreats.

To more effectively deal with cyber events, the National Institution of Standards and Technology (NIST) provides a policy framework of computer security guidance for how organizations can assess and improve their ability to prevent, detect, and respond to cyberattacks. This framework is an industry accepted methodology for building a plan to develop and implement safeguards to ensure delivery of critical business services.

As shown in the Figure 1, a Cyber Resilience plan is a continuous process that must be repeated in the environment to safeguard the data from the cyber attacks.



Figure 1 NIST Cyber Security framework

The framework consists of the following set of Cyber Security functions:

- Identify: NIST recommends building organizational understanding during Identify stage so that business IT systems can be confidently restored to their operational state. It is important to identify what must be protected and prioritize the protection plan.
- Protect: During the Protect stage, implement safeguards, such as identity management, access control, awareness and training, data security, code currency procedures, and data protection technology to ensure delivery of critical services.
- Detect: The best way to reduce costs during an event is to detect it early and rapidly recover. The point of the Detect stage is to implement activities and technologies to identify anomalies and events that are out of the ordinary to quickly respond and limit the damage by containing the event.
- Respond: In this Response state, suitable activities are developed and implemented to take actions regarding a detected cybersecurity incident.
- Recover: In Recover stage, suitable activities are developed and implemented to maintain plans for resilience and to restore any capabilities or services that were impaired because of a cybersecurity incident. The goal is to get the compromised environment up and running quickly and efficiently.

Implementing Hybrid Cloud Cyber Resilience Solution with IBM Spectrum Protect Plus and IBM Cloud Object Storage

This section describes the components and solution building blocks that used for implementing the Hybrid cloud Cyber Resilience solution with IBM Cloud as a public cloud. Although IBM FlashSystem is used for storing on-premises storage, this solution can be implemented by using any supported storage system by IBM Spectrum Protect Plus.

IBM FlashSystem

The new IBM FlashSystem family (now including IBM Storwize®) simplifies storage for hybrid cloud. With a unified set of software, tools, and APIs, our hybrid flash, and all flash array storage address the entire range of storage needs from one data platform that extends enterprise functions throughout your storage estate.

IBM FlashSystem is an all flash storage virtualization to manage mixed environments and consolidated workloads. IBM FlashSystem combines the performance of flash and NVMe with the reliability and innovation of IBM FlashCore® and the rich features of IBM Spectrum Virtualize. This feature brings high-end capability to clients that need enterprise mid-range storage and multicloud storage and offers NVMe and multicloud ultra-high throughput storage system.

IBM Spectrum Protect Plus

IBM Spectrum Protect Plus is a modern data protection solution that provides near-instant recovery, replication, retention, and reuse for VMs, databases, and containers in hybrid multicloud environments. It is easily deployed as a virtual appliance and the agentless architecture is easy to maintain. It also unlocks the value of your data by improving the quality and speed of development, testing, and analytics.

IBM Spectrum Protect Plus offers cost-effective data retention, data compliance, and disaster recovery by way of data offload to on-premises and cloud-based Object Storage and IBM Spectrum Protect, including support for the physical and virtual tape. IBM Spectrum Protect's integration with IBM Cloud Object Storage offers protection against cyber attacks by storing copies in immutable mode inside IBM Cloud Object Storage WORM buckets.

IBM Cloud Object Storage

IBM Cloud Object Storage makes it possible to store an almost limitless amount of data easily and cost effectively. It is commonly used for data archiving and backup; for web and mobile applications; and as scalable, persistent storage for analytics. Flexible storage class tiers with a policy-based archive allow you to effectively manage costs while meeting data access needs.

The integrated IBM Aspera® high-speed data transfer option makes it easy to transfer data to and from IBM® Cloud Object Storage. The query-in-place function allows you to run analytics directly on your data.

IBM Cloud® Object Storage supports exponential data growth and cloud-native workloads. With built-in high-speed file transfer capabilities, cross-region offerings, and integrated services, IBM Cloud Object Storage can help you securely use your data.

IBM Cloud

IBM Cloud offers the most open and secure public cloud for business, a next-generation hybrid cloud platform, advanced data and AI capabilities, and deep enterprise expertise across 20 industries. A full stack cloud platform with over 170 products and services covers data, containers, AI, IoT, and blockchain.

Use cases considered for Cyber Resilience Solution across hybrid cloud

The architectural design in this cyber resilience solution addresses following use cases:

- As a storage architect and administrator, data should be safeguarded from virus attacks, ransomware encryption, or deletion by a malicious user.
- As a storage architect and admin, data is at-most important and business of organization relies on the data on the storage system. Business can continue, even if the data on the primary system that is holding the data was compromised.
- Multiple copies of data are maintained by using multiple features of data protection, even if of one or more copies of data are compromised.
- Copies of data are available in immutable format to avoid overriding of valid copies of data.
- Ability to restore valid copies of data to a remote system to validate the authenticity of recovered data.
- Copies of data are stored in an air-gapped environment where only authorized personal can access it.

Avoid human elements from accessing and compromising all copies of data, with provision to store multiple copies of data at different locations and separating administrative access for the different copies of data.

Establish site-to-site IPSec VPN for hybrid-cloud connectivity with IBM Cloud

This section provides an overview of hybrid cloud connectivity between the IBM Cloud site and the on-premises site (see Figure 2). It also describes how to configure the site-to-site IPSec tunnel for communication between IBM Cloud and the on-premises site.

Note: Although this section describes the logical steps for the use case that is shown, the on-premises network configuration, infrastructure, and security policy can vary on a case-by-case basis. This section is intended to give a high-level logical overview.

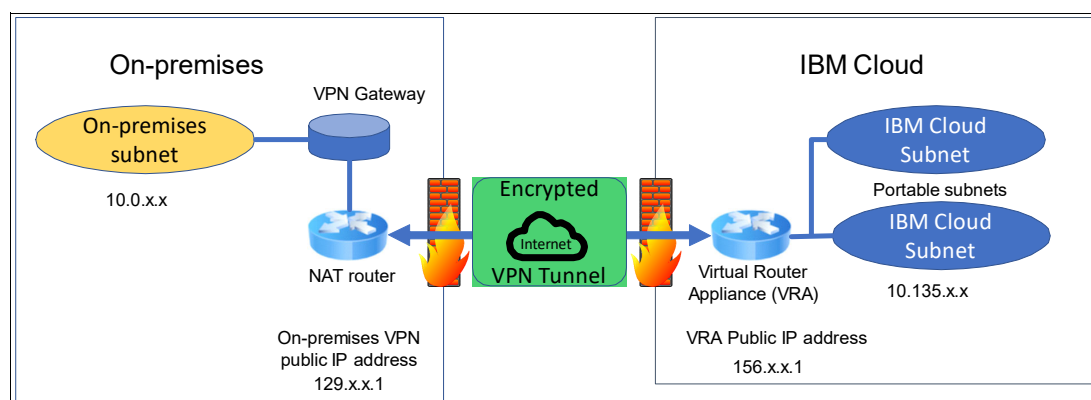


Figure 2 IPSec VPN tunnel overview

As shown in Figure 2, IBM Cloud uses Virtual Router Appliance (VRA), which acts as a default router for the private and portable private subnets. All of the compute hosts and applications are configured with IP addresses in the portable IP subnets.

At the on-premises site, a network address translation (NAT) router is used with public IP address. That public IP address is NAT'ed to a private IP subnet address.

This VPN IPsec site-to-site tunnel creates a secure communication network between your IBM Cloud infrastructure and on-premises infrastructure. Network communication between the private subnets is controlled by the access control list that is populated when the VPN IPsec site-to-site tunnel is created.

Architectural overview of Hybrid Cloud Cyber Resilience solution

Figure 3 shows the high-level architectural overview of hybrid cloud cyber resilience solution for protecting data that is on IBM FlashSystem® or any other supported storage system using IBM Spectrum® Protect Plus and IBM Cloud Object Storage.

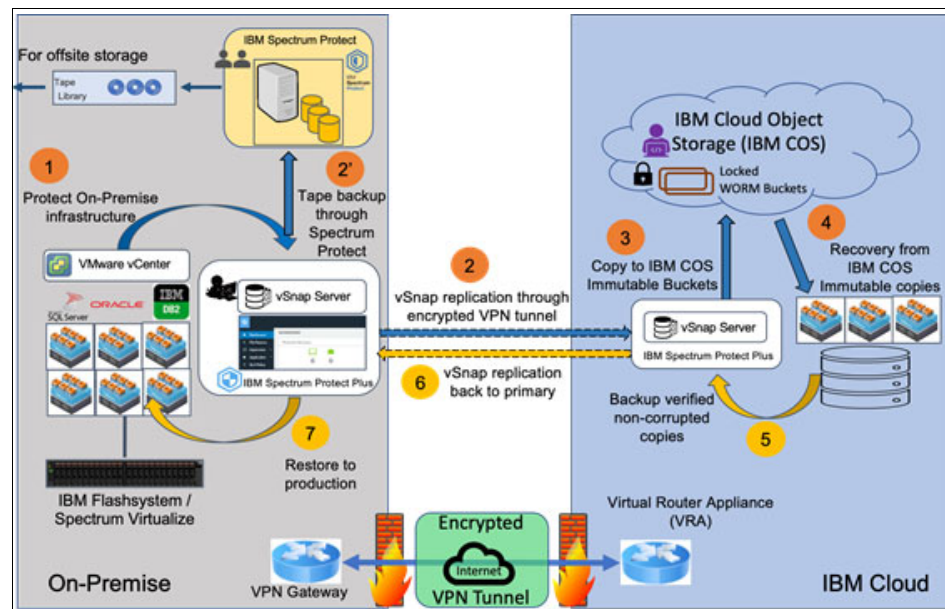


Figure 3 Hybrid Cloud Cyber Resilience Solution - Architectural overview

In this proof of concept and solution validation, VMware infrastructure (including VMware vCenter Server and VMware vSphere) are configured by using IBM FlashSystem. VMware infrastructure is running Microsoft SQL Server on a virtual machine, which uses storage from IBM FlashSystem. IBM Spectrum Protect Plus server is configured in the on-premises data center along with local vSnap server.

Inside IBM cloud, VMware ESXi server infrastructure was purchased and configured. Another vSnap server is configured on IBM Cloud and was used as remote vSnap server to replicate protected data from on-premises vSnap server by using the vSnap replication feature.

The VMware infrastructure inside IBM Cloud is also used to restore immutable copies from IBM Cloud Object Storage WORM buckets. These immutable copies are non-tampered copies of production data and can be used to restore copies and validate them inside IBM Cloud to verify data integrity and non-corruption due to cyberattacks.

IBM Cloud infrastructure can also be used for maintaining business continuity and disaster recovery use cases. If any unintended event occurs to the primary data center or infrastructure, the entire workload can be failed over to the IBM Cloud infrastructure by restoring copies from IBM Cloud Object Storage or remote vSnap server that is inside IBM Cloud.

IBM Cloud Object Storage was also purchased to be used inside IBM Cloud to create WORM buckets. IBM Cloud Object Storage WORM buckets are used to copy data from remote vSnap server. IBM Spectrum Protect Plus allows data to be copied always in incremental mode from remote vSnap server and in archival mode in immutable format. If any cyber events occur, immutable copies of IBM Spectrum Protect Plus can restore data from IBM Cloud Object Storage in “test” or “clone” mode to verify the restored copies that they are not tampered with by cyber attacks.

As a best practice and to safeguard against manual cyber events, administrative controls for all involved components, such as IBM Spectrum Protect Plus and IBM Cloud Object Storage should be maintained separately. After the protected data is copied over to IBM Cloud Object storage immutable buckets, those copies cannot be deleted until the retention policy on the WORM buckets expires.

Considerations

Consider the following points:

- IBM Cloud Object Storage in IBM Cloud allows you to design Single Site, Regional, or multi-site configurations. This configuration can be implemented based on the feasibility and business that is need to maintain copies across single, regional, or multi-sites for better protection against cyber-events.
- On-premises and IBM Cloud site should be configured per the requirements and options that are provided by IBM Cloud. I/O latency and bandwidth between on-premises and IBM Cloud should be considered for replicating data across hybrid cloud and deciding on recovery point objectives (RPO) and recovery time objectives (RTO).
- IBM Spectrum Protect Plus allows setting up multiple configurations by using multiple vSnap servers. This configuration can be implemented based on the feasibility and business that is need to maintain multiple copies of data. In this solution validation, only one on-premises and remote vSnap server is considered.
- If IBM Cloud Object Storage is directly accessible from on-premises IBM Spectrum Protect Plus server, restores from IBM Cloud Object Storage WORM buckets can directly be performed to the primary site.

Site-to-site IPsec VPN tunnels were established between on-premises infrastructure with IBM Cloud infrastructure. After the IPsec VPN tunnel is established and configured, on-premises and IBM Cloud setup can communicate with each other to replicate and protect the data from cyber events.

Optionally, IBM Spectrum Protect Plus also can archive IBM Spectrum Protect Plus protected data to an IBM Spectrum Protect server for enhanced cyber resilience purposes. IBM Spectrum Protect can use tapes for copying weekly, monthly, or less frequent full copy of data from IBM Spectrum Protect Plus.

When data is copied to tape, a full copy of the data is created at the time of the copy process. Copying data to tape provides extra security benefits. By storing tape volumes at a secure, off-site location that is not connected to the internet, you can help to protect your data from online threats, such as malware and hackers.

However, because copying to these storage types requires a full data copy, the time that is required to copy data increases. In addition, the recovery time can be unpredictable, and the data might take longer to process before it is usable.

For more information, see the “Configuration for copying or archiving data to IBM Spectrum Protect” section of [IBM Knowledge Center](#).

Setting up Hybrid Cloud Cyber Resilience solution

This solution approach is designed by using standard software components of IBM Spectrum Protect Plus, and IBM Cloud Object Storage on IBM Cloud.

On-premises setup and configuration

For this proof of concept and solution validation, on-premises infrastructure was configured inside IBM lab with access to the public network for hybrid cloud connectivity with IBM Cloud over the IPsec VPN tunnel.

Note: All the configurations that are described in this solution proof of concept are for illustration purpose only. Actual configurations vary in a real environment and must plan based on RPO and RTO and bandwidth considerations for connectivity between on-premises and an IBM Cloud environment.

The following components were installed and configured inside IBM lab:

- IBM FlashSystem
- VMware vSphere 6.7 for hosting virtual machines
- VMware vCenter Server 6.7
- IBM Spectrum Protect Plus server 10.1.6 with vSnap server
- Microsoft SQL Server 2012 on a Windows virtual machine
- VyOS appliance for hybrid cloud network connectivity

VMware vSphere on IBM FlashSystem

For this IBM Blueprint, VMware infrastructure was configured on IBM FlashSystem 9100 by using a storage area network (SAN) configuration. VMware ESXi server 6.7 along with VMware vCenter server 6.7 was installed and configured per best practices.

IBM FlashSystem 9100 storage was configured per best practices and connected to SAN fabric. IBM FlashSystem 9100 volume was configured and assigned to VMware ESXi server over Fibre Channel network.

For this solution validation and database application validation, Microsoft SQL Server was installed and configured on a Windows virtual machine. Any IBM Spectrum Protect Plus supported back-end storage system can be used based on application compatibility.

For more information about installation and configuration of IBM FlashSystem, see the documentation that is available at [IBM Knowledge Center](#).

IBM Spectrum Protect Plus with vSnap server

For the validation of this solution, IBM Spectrum Protect Plus Server along with vSnap server was deployed on a separate VMware ESXi server. For more information and supported configurations, see IBM Spectrum Protect Plus Blueprints.

After installation, follow the best practices that are specified in [IBM Knowledge Center](#) (search for “configure IBM Spectrum Protect Plus server and on-premises vSnap server”) to configure IBM Spectrum Protect Plus server and on-premises vSnap server.

IBM Cloud setup and configuration

For this solution validation, the necessary equipment was purchased and setup inside the IBM Cloud location that was near to the IBM lab where on-premises setup was performed. For purchasing and setting up equipment in IBM Cloud, IBM Cloud registration is required.

For more information, see [this web page](#).

For this proof of concept and solution validation, the following equipment was set up inside IBM Cloud:

- VMware vSphere ESXi 6.7 server for restoring virtual machines
- IBM Spectrum Protect Plus vSnap server
- IBM Cloud Object Storage
- Virtual Router Appliance for hybrid cloud connectivity with IBM lab

VMware vSphere ESXi server setup in IBM Cloud

For the scope of this proof of concept and solution validation, VMware ESXi server was purchased and setup in IBM Cloud.

Complete the following steps:

1. Log in to IBM Cloud account and go to VMware Solutions and select **VMware Solutions Dedicated**. Then, select the VMware vSphere server instance per the requirements (see Figure 4).

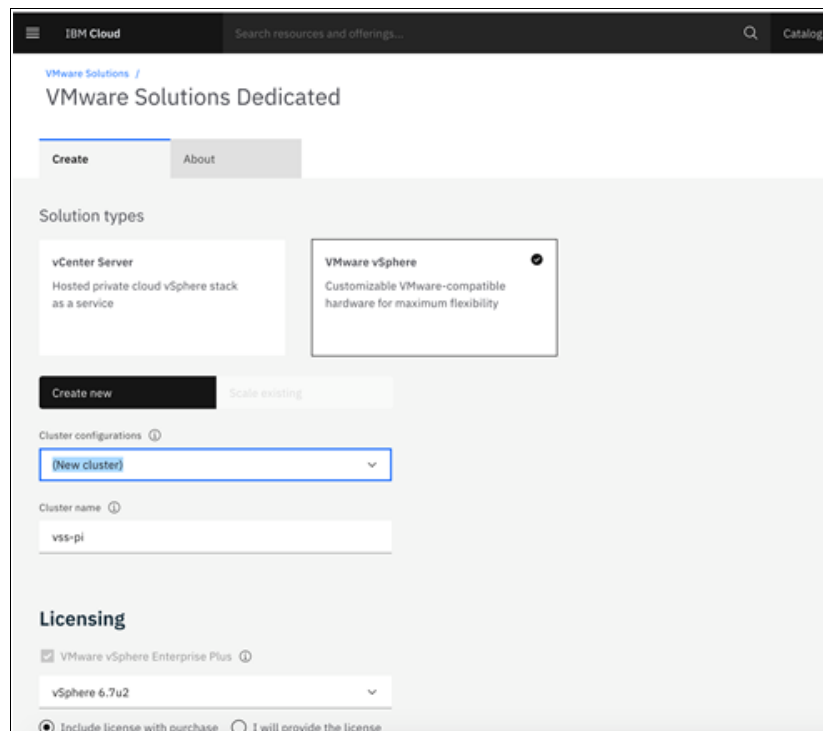


Figure 4 VMware Infrastructure purchase in IBM Cloud

2. Select and purchase the required storage from IBM Cloud and connect it to the VMware ESXi server for validating non-corrupted copies restore inside IBM Cloud from IBM Cloud Object Storage WORM buckets.

Installing vSnap Server in IBM Cloud

vSnap server in IBM Cloud can be deployed by using the following methods:

- A Linux operating system that supports manual vSnap installations is required to install a vSnap server on a virtual or physical machine.
- vSnap server can be installed in a VMware virtual infrastructure by using the Open Virtualization Format (OVA) template. This method creates a machine that includes the vSnap server.

For this proof of concept and solution validation, vSnap server was installed in a VMware virtualized environment by using the OVA template. For more information about instructions for setting up vSnap server in a virtualized environment, see [IBM Knowledge Center](#) and search for “Installing vSnap servers section”.

IBM Cloud Object Storage setup and configuration in IBM Cloud

For this proof of concept and solution validation, IBM Cloud Object Storage instance was purchased in IBM Cloud. For purchasing IBM Cloud Object Storage instance, use your registered account with IBM Cloud.

Complete the following steps:

1. Log in to IBM Cloud account and select **Storage resources** → **Create resource**. Select **Object Storage**. On the next page, enter the Service name for your IBM Cloud Object Storage instance and then, select **Create** to create and add IBM Cloud Object Storage instance to your account (see Figure 5).

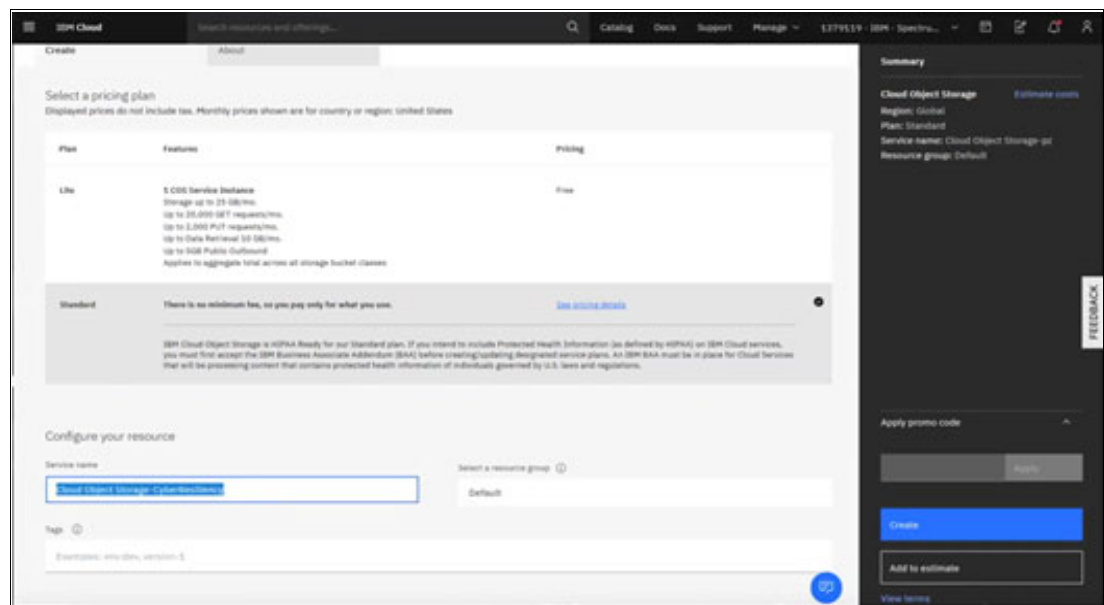


Figure 5 IBM Cloud Object Storage instance purchase in IBM Cloud

The new IBM Cloud Object Storage instance is displayed under Storage resources (see Figure 6).

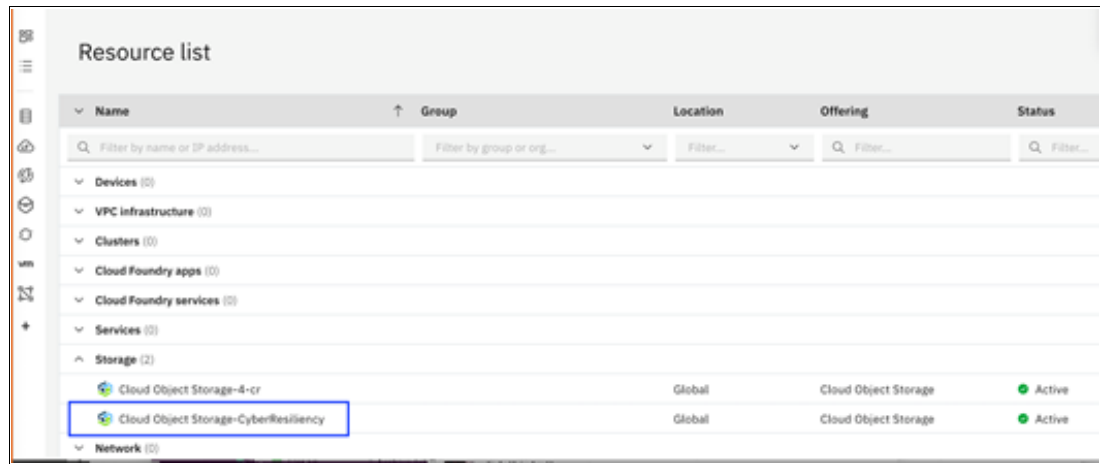


Figure 6 IBM Cloud Object Storage instance displayed

- For the newly created IBM Cloud Object Storage instance, make note of the private and public endpoints by browsing to Endpoint. These endpoints are needed while configuring IBM Cloud Object Storage instance in IBM Spectrum Protect Plus configuration (see Figure 7).

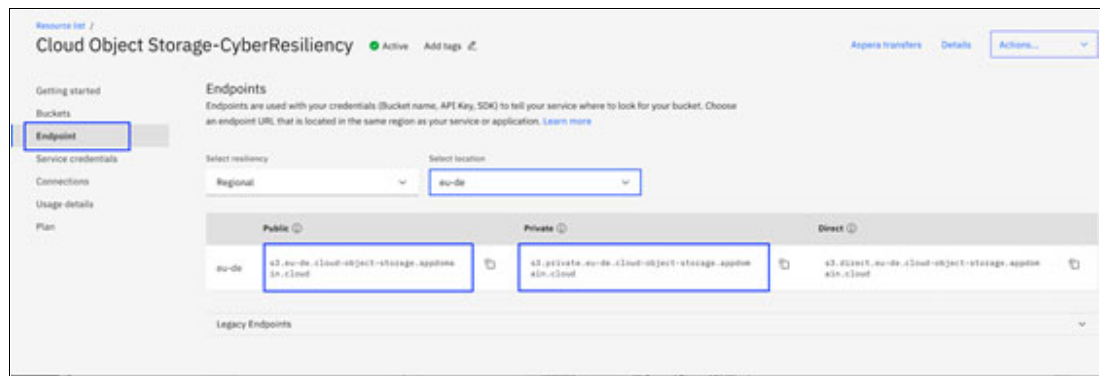


Figure 7 IBM Cloud Object Storage instance endpoints in IBM Cloud

- IBM Cloud Object Storage credentials must be created for IBM Cloud Object Storage instance. For creating IBM Cloud Object Storage credentials, select **Service credentials** → **New credential** (see Figure 8).

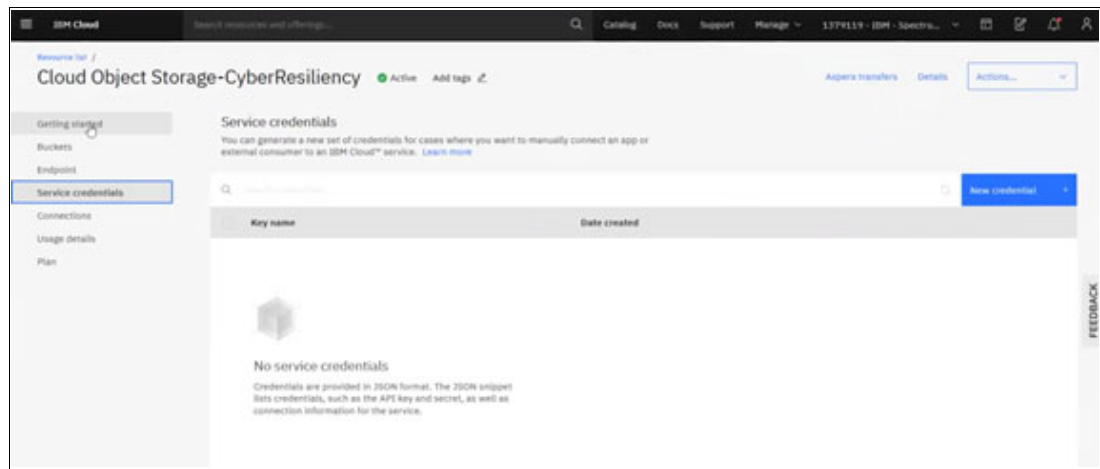


Figure 8 Creating IBM Cloud Object Storage service credentials in IBM Cloud

- Enter the name for the IBM Cloud Object Storage credentials, select **Writer** as the Role and **Auto Generate** as the Service ID. Then, select **On** for the Include HMAC Credential. Then, click **Add** to create the IBM Cloud Object Storage credentials (see Figure 9).

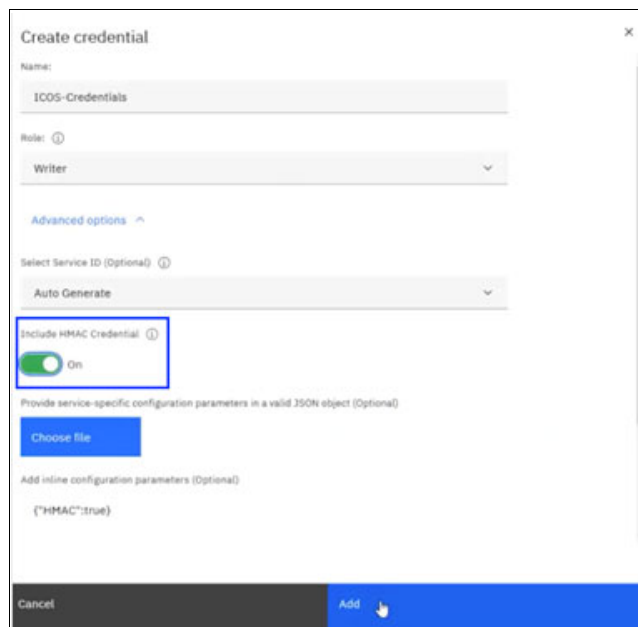


Figure 9 Creating IBM Cloud Object Storage credentials details

5. New IBM Cloud Object Storage credentials are generated. Browse to Service credentials and make a note of the access_key_id and secret_access_key from the credentials (see Figure 10). This information is needed to configure IBM Cloud Object Storage storage inside IBM Spectrum Protect Plus storage options.

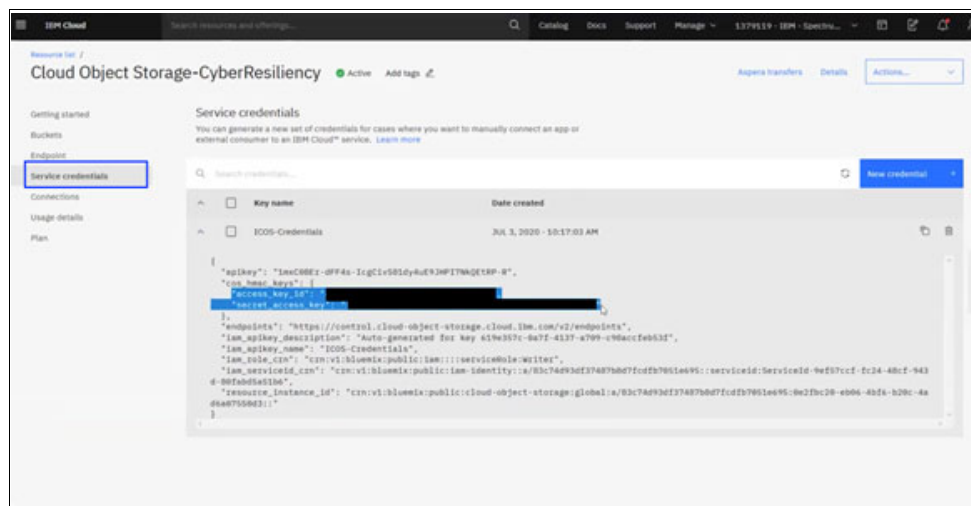


Figure 10 Listing of IBM Cloud Object Storage service credentials

For cyber resilience for this solution and to store copies of data that is protected by IBM Spectrum Protect Plus in immutable format, WORM buckets are created in IBM Cloud Object Storage instance.

After protected copies are copied to WORM buckets in IBM Cloud Object Storage, these copies cannot be deleted unless the retention period on these buckets expires. This feature helps organizations to store copies of data in an object format that cannot be tampered with, and in an environment that is managed and administered by separate administrators than the primary storage administrator (in this case IBM FlashSystem) or primary data protection software administrator (in this case IBM Spectrum Protect Plus).

Therefore, this separation helps protect copies of data against internal cyber events, such as administrator accidentally or purposefully trying to delete data from your primary environment.

6. To create IBM Cloud Object Storage WORM buckets, click **Buckets** → **Custom bucket** to start creating a bucket to store unstructured data.

7. In the Custom bucket wizard, enter a unique name for IBM Cloud Object Storage WORM bucket. Select **Resiliency** from the options Cross Region, Regional, or Single Site based on the preference. For this solution validation, the **Regional resiliency** option is selected for faster copying of data to IBM Cloud Object Storage instance. Then, select the preferred Storage class. For this solution validation, the **Standard** option was selected (see Figure 11).

The screenshot shows the IBM Cloud console interface for creating a custom bucket. The page title is "Cloud Object Storage-CyberResiliency" with a green "Active" status and an "Add tags" link. The "Custom bucket" section includes a text input for the "Unique bucket name" containing "spp-icos-worm-11days". Below this is a blue information box titled "Bucket naming rules:" with a close button (X). The rules listed are: "Must be unique across the whole IBM Cloud Object Storage system", "Do not use any personal information (any part of a name, address, financial or security accounts or SSN)", "Must start and end in alphanumeric characters (3 to 63)", and "Characters allowed: lowercase, numbers and non-consecutive dots and hyphens". The "Resiliency" section has three options: "Cross Region" (Highest availability), "Regional" (Best performance, selected with a blue checkmark), and "Single Site" (Data sovereignty). The "Location" dropdown menu is set to "eu-de". The "Storage class" section has two options: "Smart Tier" (marked as "New") and "Standard" (selected with a blue checkmark). The "Standard" option description reads: "For active workloads that require higher performance and low latency and where data needs to be accessed frequently." There is a "View pricing" link next to the storage class options.

Figure 11 Create WORM buckets in IBM Cloud Object Storage

8. Add an Expiration rule for the object. Setting the object expiration rule results in cost savings by scheduling the deletion of objects that are no longer needed after a specified amount of time.

Select **Expiration** → **Add rule** (see Figure 12 on page 15). Enter the Rule name and specify Expiration days and then, click **Save** to set the expiration rule on the objects of the IBM Cloud Object Storage WORM bucket.

Figure 12 Set expiration rule on the WORM buckets

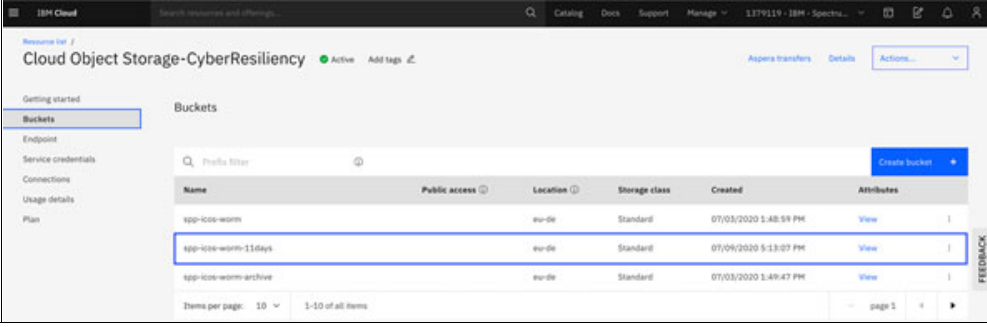
9. Select **Retention policy** for the bucket to create the retention policy to prohibit deletes and overwrites of the objects inside the bucket. This selection helps to protect copies of data, which prohibits overwriting the data that is inside IBM Cloud Object Storage if cyber events occur at the primary site and data is corrupted by cyberattacks or ransomware attacks at primary site.

Select the retention period and click **Save** to save the Retention policy (see Figure 13).

Figure 13 Set Rules and retention policies for WORM buckets

10. After specifying the necessary configuration for the bucket, click **Create bucket** to create WORM bucket.

The new IBM Cloud Object Storage bucket is configured with the specified configuration on IBM Cloud Object Storage instance inside IBM Cloud (see Figure 14).



The screenshot shows the IBM Cloud console interface. On the left, there's a sidebar with navigation options: Getting started, Buckets (selected), Endpoint, Service credentials, Connections, Usage details, and Plan. The main area is titled 'Cloud Object Storage-CyberResiliency' and shows a 'Buckets' section. A table lists the buckets with columns: Name, Public access, Location, Storage class, Created, and Attributes. The buckets listed are 'app-ico-worm', 'app-ico-worm-11days', and 'app-ico-worm-archive'. The 'app-ico-worm-11days' bucket is highlighted with a blue border. At the bottom of the table, it says 'Items per page: 10' and '1-10 of all items'. There's also a 'page 1' indicator.

Name	Public access	Location	Storage class	Created	Attributes
app-ico-worm		eu-de	Standard	07/03/2020 1:48:59 PM	View
app-ico-worm-11days		eu-de	Standard	07/04/2020 5:13:07 PM	View
app-ico-worm-archive		eu-de	Standard	07/03/2020 1:49:47 PM	View

Figure 14 IBM Cloud Object Storage instance buckets listing

IBM Cloud Object Storage configuration in IBM Spectrum Protect Plus

After the IBM Cloud Object Storage instance is configured and set-up in IBM Cloud, it must be registered in IBM Spectrum Protect Plus. For more information about the prerequisites for adding IBM Cloud Object Storage as a backup storage provider, see [IBM Knowledge Center](#) and search for “adding IBM Cloud Object Storage as a backup storage provider”.

Complete the following steps:

1. In IBM Spectrum Protect Plus graphical user interface (GUI), select **System Configuration** → **Backup Storage** → **Object Storage**. Select **Add Object Storage**.
2. From the provider list, select **IBM Cloud Object Storage**, as shown in Figure 15.

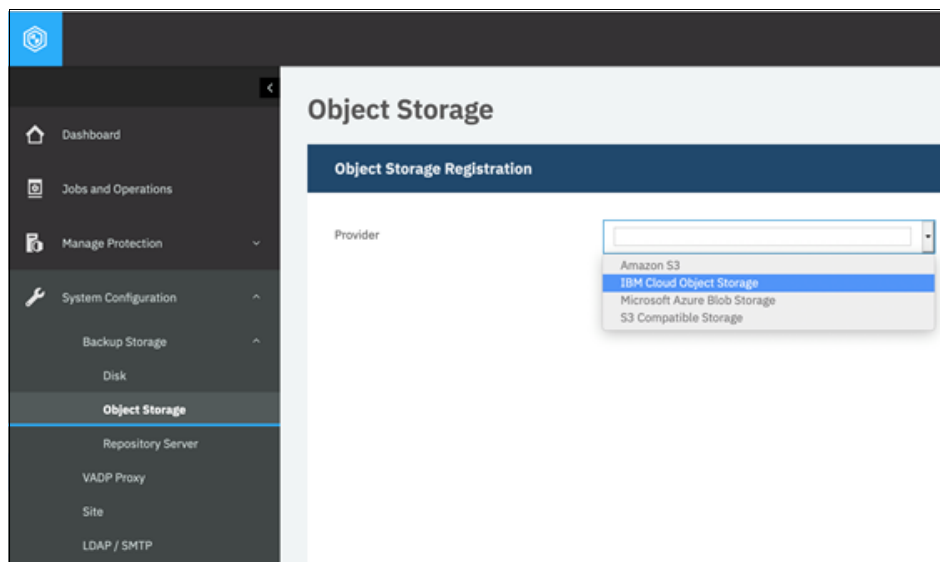


Figure 15 IBM Cloud Object Storage configuration in IBM Spectrum Protect Plus

3. In IBM Cloud Object Storage registration window, enter the name of the IBM Cloud Object Storage provider, select the Endpoint that was noted when the IBM Cloud Object Storage instance inside IBM Cloud was created.

- Enter the unique Key name, Access key, and Secret key that were noted from IBM Cloud Object Storage instance inside IBM Cloud. A certificate is not required while adding public IBM Cloud Storage instance. For this solution validation, we use IBM Cloud Storage instance inside IBM Cloud. Therefore, a certificate is not required (see Figure 16).

Figure 16 Configure IBM Cloud Object Storage endpoints and credentials

- Click **Get Buckets**. Select the WORM bucket that was created in IBM Cloud Object Storage storage instance inside IBM Cloud as a Standard object storage bucket (see Figure 17).

Figure 17 Specify IBM Cloud Object Storage WORM buckets in IBM Spectrum Protect Plus

Optionally, select the Archive object storage bucket that can be used to create full data copies and provide long-term data protection. To use an archive object storage bucket for long-term data protection inside IBM Cloud, this bucket must be created in the IBM Cloud Object Storage in advance because we cannot use the same bucket for Standard *and* Archive purposes.

6. Click **Register** to register IBM Cloud Object Storage storage instance in IBM Spectrum Protect Plus. It is displayed under Object Storage Servers (see Figure 18).

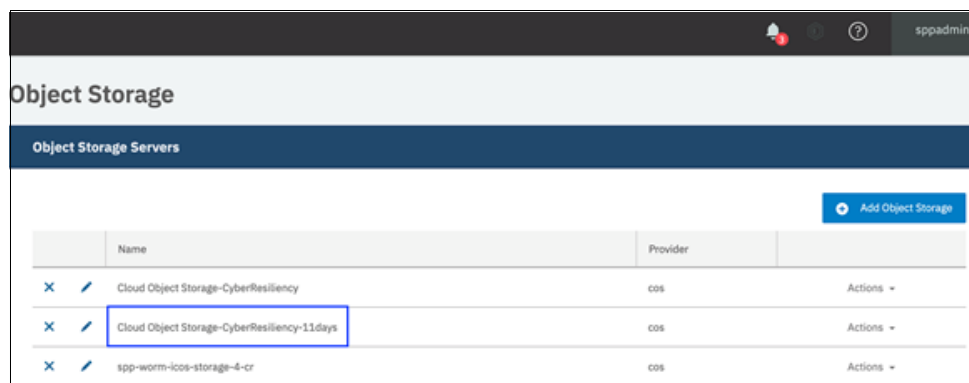


Figure 18 IBM Cloud Object Storage listing in IBM Spectrum Protect Plus

Creating a Cyber Resilience SLA policy in IBM Spectrum Protect Plus

After an IBM Cloud Object Storage instance is configured in IBM Spectrum Protect Plus, create a cyber resilience service level agreement (SLA) policy in IBM Spectrum Protect Plus. This policy is used to back up the data to primary vSnap server; then, replicate the protected data to remote vSnap server and finally, copy the protected data to IBM Cloud Object Storage storage instance to protect the copies in immutable format by using WORM buckets in IBM Cloud Object Storage instance inside IBM Cloud.

Complete the following steps:

1. To create cyber resilience policy, select **Manage Protection** → **Policy Overview**. Then, scroll down to SLA Policies and click **Add SLA Policy** to start creating a cyber resilience SLA policy in IBM Spectrum Protect Plus GUI.
2. In the New SLA Policy window, enter a unique name and select type of backup. In the backup policy section, select the backup retention. Every organization must select retention based on its own SLA policies. Typically, backups are scheduled to run per a backup schedule. If it is not required, disable the schedule by checking the option. Select the Frequency, Start Time. Select the Target Site as **Primary** because the primary backup location is local vSnap server (see Figure 19 on page 19).

Policy Overview

New SLA Policy

Name: CR-SPP-IC05-11days

☒ VMware, Hyper-V, Exchange, Office365, SQL, Oracle, DB2, MongoDB, Catalog, and Windows File Systems

☐ Kubernetes

☐ Amazon EC2

Backup Policy

Retention: 11 Days

☐ Disable Schedule

Frequency: 1 Days

Start Time: 07/09/2020 01:00 Europe/Berlin

Target Site: Primary

☐ Only use encrypted disk storage.

Replication Policy

☐ Backup Storage Replication

☒ Disable Schedule

Cancel Save

Figure 19 Create new Cyber Resilience SLA policy in IBM Spectrum Protect Plus

3. In the same New SLA Policy window in the Replication Policy section, select **Backup Storage Replication** and select the remote vSnap server (in this case, **IBM-Cloud**) as Target Site. For our example, we selected **Same retention** as source retention selection (see Figure 20).

Policy Overview

New SLA Policy

☐ Disable Schedule

Frequency: 1 Days

Start Time: 07/09/2020 01:00 Europe/Berlin

Target Site: Primary

☐ Only use encrypted disk storage.

Replication Policy

☒ Backup Storage Replication

☐ Disable Schedule

Frequency: 1 Days

Start Time: 07/09/2020 03:00 Europe/Berlin

Target Site: IBM-Cloud

☐ Only use encrypted disk storage.

☒ Same retention as source selection.

Retention: 11 Days

Cancel Save

Figure 20 Configure replication in new Cyber Resilience SLA policy

4. Scroll down further and select **Standard object storage (incremental copy)** in the Additional Copies section. Select from where data is copied to IBM Cloud Object Storage immutable buckets. In this example, we are coping the data from remote vSnap server. Select **Destination** as Cloud services.

5. Select Target as immutable IBM Cloud Object Storage storage instance configured on IBM Spectrum Protect Plus from the drop-down list. In this technical paper, we are selecting retention period **Same retention** as source selection (see Figure 21).

The screenshot shows the 'New SLA Policy' configuration interface. It includes sections for 'Additional Copies' and 'Archive object storage (full copy)'. The 'Additional Copies' section is active, showing a frequency of 1 day and a start time of 07/04/2020 05:00. The 'Target' dropdown is open, showing options like 'Cloud Object Storage-CyberResiliency' and 'Cloud Object Storage-CyberResiliency-11days'. The 'Retention' dropdown is also open, showing 'Same retention as source selection' as the selected option.

Figure 21 Configure copy to IBM Cloud Object Storage in new Cyber Resilience SLA policy

Optionally, select Archive object storage (full copy) to be made from remote vSnap server to IBM Cloud Object Storage immutable bucket.

6. After all the configuration is complete, select **Save** to create new cyber resilience SLA policy in IBM Spectrum Protect Plus (see Figure 22).

Name	Job type	Frequency	Retention
Bronze	Backup	Every 1 Days at 2:06:21 AM	1 Weeks
CR-SPP-ICDS-11days	Replication Copy	Every 1 Days at 3:00:00 AM	Same retention as source selection.
	Backup	Every 1 Days at 5:00:00 AM	Same retention as source selection.
	Backup	Every 1 Days at 1:00:00 AM	1.1 Days
CR-To-ICDS-Policy	Replication	Schedule Disabled	Same retention as source selection.
	Copy	Schedule Disabled	Same retention as source selection.
	Archive	Schedule Disabled	1 Months
	Backup	Schedule Disabled	1 Weeks
CyberResiliency-Policy	Replication	Schedule Disabled	Same retention as source selection.
	Copy	Schedule Disabled	Same retention as source selection.
	Archive	Schedule Disabled	1 Months
	Backup	Schedule Disabled	1 Weeks
Gold	Backup	Every 4 Hours	1 Weeks
Silver	Backup	Every 1 Days at 2:06:21 AM	1 Months

Figure 22 New Cyber Resilience SLA policy listing

Cyber Resilience Solution use cases

The following use cases were considered for this technical paper.

- Protect the VMware virtual machine data that is installed on your primary storage through IBM Spectrum Protect Plus in a WORM bucket of IBM Cloud Object Storage to protect it against cyber events.

- Restore a virtual machine from immutable buckets of IBM Cloud Object Storage in IBM Cloud location. This virtual machine can be restored in a test, clone, or production mode.
- After verifying non-corrupted copy of a virtual machine that is restored from IBM Cloud Object Storage, restore back the virtual machine to the primary site.
- Protect SQL Server database instance through IBM Spectrum Protect Plus in a WORM bucket of IBM Cloud Object Storage to protect against cyber events.
- Restore SQL Server database instance from immutable buckets of IBM Cloud Object Storage inside IBM Cloud location.

Protecting virtual machine data to IBM Cloud Object Storage WORM buckets

To protect data from cyber events, it must be protected in read-only and tampered proof storage. We use IBM Cloud Object Storage WORM buckets as read-only storage instance.

To protect data to IBM Cloud Object Storage, the following operations were considered:

- Protecting the data from virtual infrastructure to primary vSnap server inside the same primary site.

This operation helps in instant recovery in a virtualized environment. However, you cannot fully rely on the backups at primary vSnap server because chances exist that the entire primary site can be compromised if a cyber event occurs.

- Replication of protected data at primary vSnap server to the remote vSnap server.

This operation is a good practice of replicating protected data inside IBM Spectrum Protect Plus to another location. It helps in disaster recovery and business continuity use cases, and enables business operations at secondary site. However, you cannot guarantee that protected data at vSnap server is tamper-proof from internal and external cyber events.

- Copying protected data from secondary vSnap server to WORM buckets of IBM Cloud Object Storage for protection against cyber events.

This configuration provides the highest level of protecting data against internal and external cyber events. In this case, IBM Spectrum Protect Plus administrator can copy and restore only the data to IBM Cloud Object Storage WORM buckets. They cannot access the data that is inside IBM Cloud Object Storage because it is stored in an object format.

Also, after the retention policy is set on the IBM Cloud Object Storage WORM buckets, those objects cannot be deleted by IBM Cloud Object Storage administrators. This helps in preventing internal cyber events. Copies of data from vSnap server to IBM Cloud Object Storage also are always incremental. After those copies are written in WORM buckets, they cannot be overwritten. Therefore, this helps in protecting the data from external cyber events.

Protecting the data to primary vSnap server

Before protecting virtualized systems, they must be registered in IBM Spectrum Protect Plus and then the back-up job must be created in IBM Spectrum Protect Plus. In our example, we use cyber resilience SLA policy to backup virtualized system:

1. To create a backup job, in IBM Spectrum Protect Plus GUI, select **Manage Protection** → **Virtualized Systems** → **VMware**.
2. Select the resources to back up. In this example, we use the sql-server virtual machine to be backed up in IBM Spectrum Protect Plus.

3. Select the SLA policy and then, select the cyber resilience SLA policy that was created as described in “Creating a Cyber Resilience SLA policy in IBM Spectrum Protect Plus” on page 18.
4. Click **Save** to create the job definition by using default options.
5. The backup job runs by using the selected SLA policy. To immediately run the backup job, click **Actions** → **Start** (see Figure 23).

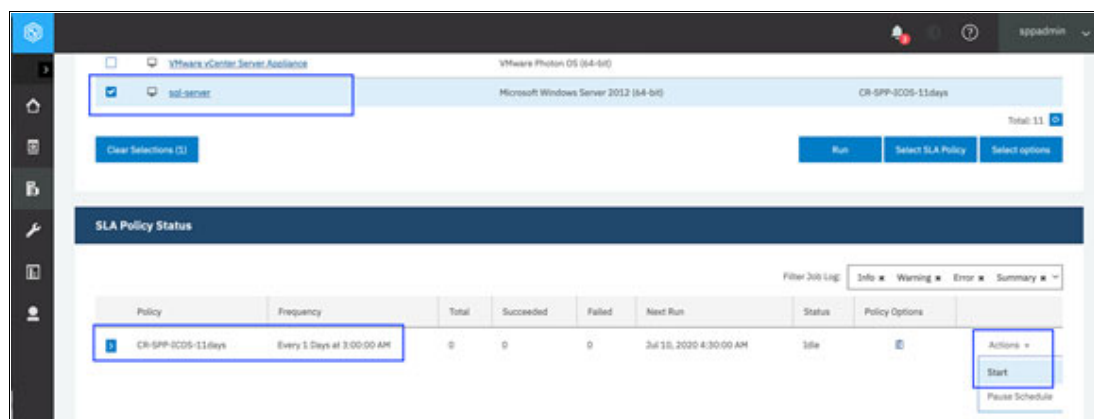


Figure 23 Start backup job from IBM Spectrum Protect Plus

6. For backing up the virtual machine to the local vSnap server first, select **Backup to vSnap** as the SLA Policy from the Start Options drop-down menu. Click **OK** (see Figure 24).

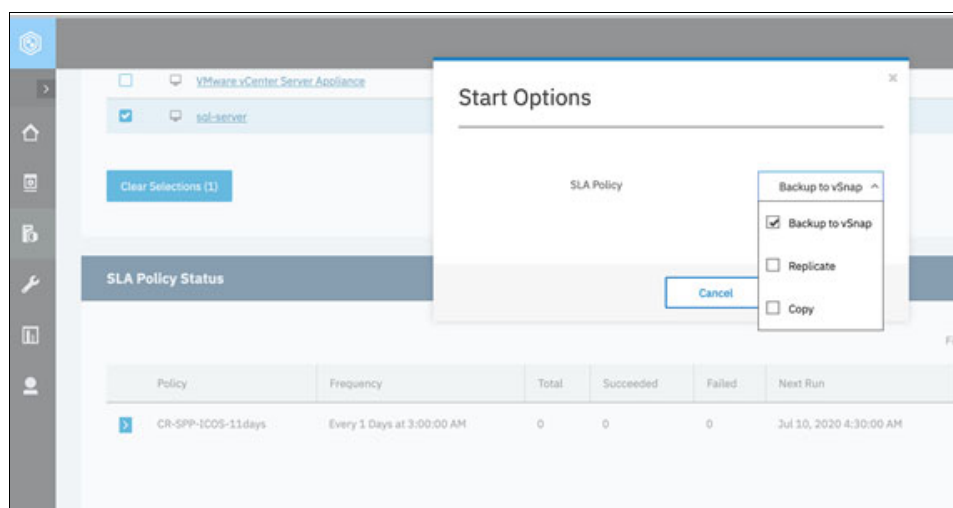


Figure 24 Selecting Backup to vSnap option in start backup job

7. Monitor the backup job by browsing to Jobs and Operations and the Running Jobs tab.

Replicating protected data to the remote vSnap server

To replicate the data from primary vSnap server to the remote vSnap server, complete the following steps:

1. in the IBM Spectrum Protect Plus GUI, select **Manage Protection** → **Virtualized Systems** → **VMware**.
2. Select the resources to back up. In this example, we use the sql-server virtual machine to be backed up in IBM Spectrum Protect Plus.

3. Select **SLA Policy** and then, select the cyber resilience SLA policy that was created as described in “Creating a Cyber Resilience SLA policy in IBM Spectrum Protect Plus” on page 18.
4. The back-up job runs by using the selected SLA policy. To immediately run the backup job, click **Actions** → **Start**.
5. For replicating the virtual machine backup from the local vSnap server to the remote vSnap server in IBM Cloud, select **Replicate** as the SLA policy from the Start Options drop-down list and click **OK** (see Figure 25).

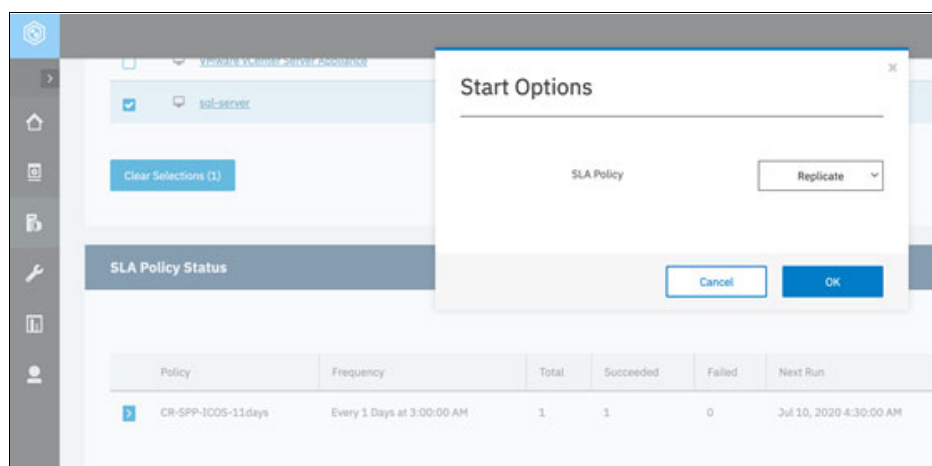


Figure 25 Start Replication job from SLA policy

6. Monitor the replication job by navigating to Jobs and Operations and in the Running Jobs tab.

Copying protected data from remote vSnap server to IBM Cloud Object Storage WORM buckets

To copy protected data from the remote vSnap server to IBM Cloud Object Storage WORM buckets from the cyber-events, complete the following steps:

1. Follow steps 1 - 4 as described in “Protecting the data to primary vSnap server” on page 21.
2. For copying the virtual machine backup from the remote vSnap server inside IBM Cloud to the IBM Cloud Object Storage WORM buckets inside IBM Cloud, select **Copy** as the SLA Policy from the Start Options drop-down list (see Figure 26 on page 24) and click **OK**.

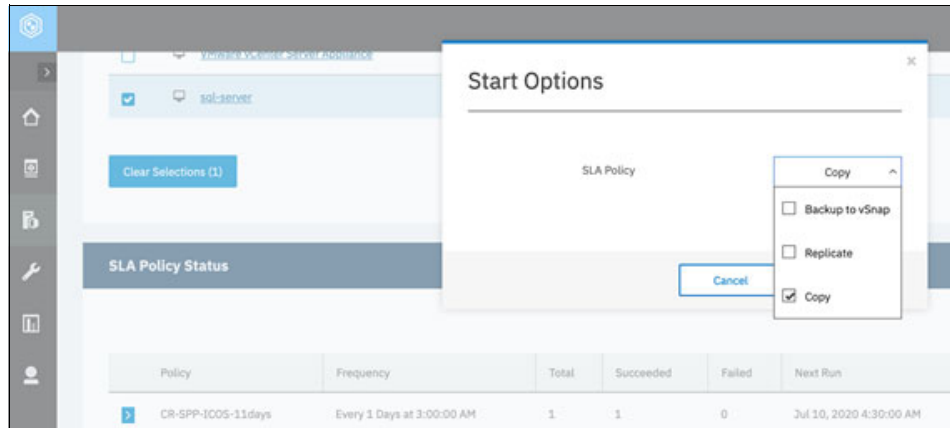


Figure 26 Start copy to IBM Cloud Object Storage in SLA policy

3. Monitor the copy job by navigating to Jobs and Operations and in the Running Jobs tab.

Recovering data from IBM Cloud Object Storage

Data recovery processes are as important as effective backup processes. If good copies are restored after a cyber event occurred, copies of data might need to be restored to verify the valid copy of data, which is a copy that was not tampered by a cyber event. In a normal restore scenario, data can be directly restored from a primary vSnap server or the remote vSnap server.

After the cyber-events occurred, it is important to know when the event occurred and then recover the non-corrupted copies from IBM Cloud Object Storage WORM buckets.

To facilitate restoring and verifying the non-corrupted copies of data, IBM Spectrum Protect Plus offers options to restore the non-tampered copies from IBM Cloud Object Storage WORM buckets in the following modes:

- Test

This mode creates temporary virtual machines for development or testing, snapshot verification, and disaster recovery verification on a scheduled, repeatable basis without affecting production environments. Test machines are kept running as long as needed to complete testing and verification and are then cleaned up.

For verifying non-corrupted copies of data, this mode might be a quick option to verify the restores. Test mode restores are served out of the vSnap storage, without the need to copy data back to a VMWare datastore.

- Clone

This mode creates copies of virtual machines for use cases that require permanent or long-running copies for data mining or duplication of a test environment in a fenced network. Virtual machines that are created in this mode are also given unique names and identifiers to avoid conflicts within your production environment. When clone mode is used, you must be sensitive to resource usage because this mode creates permanent or long-term virtual machines.

- Production

Production mode enables disaster recovery at the local site from primary storage or a remote disaster recovery site, replacing original machine images with recovery images. All configurations are carried over as part of the recovery, including names and identifiers, and all copy data jobs that are associated with the virtual machine continue to run.

For more information and prerequisites, see [IBM Knowledge Center](#) and search for “Restoring VMware data”.

Complete the following steps to recover non-corrupted data from IBM Cloud Object Storage WORM buckets:

1. To restore or verify non-corrupted copies of data inside IBM Cloud, select **Create Job** in Jobs and Operations then **Restore and VMware**.
2. On the Select Source page, select the suitable vCenter server and ESXi server and then, select the virtual machine that was protected from the primary location to protect data from cyber attacks.
3. On the Source snapshot page, select the available snapshots. In this case, we select the snapshot source as **Object Storage** and click **Next**. The read-only copies are restored from IBM Cloud Object Storage inside IBM Cloud (see Figure 27).

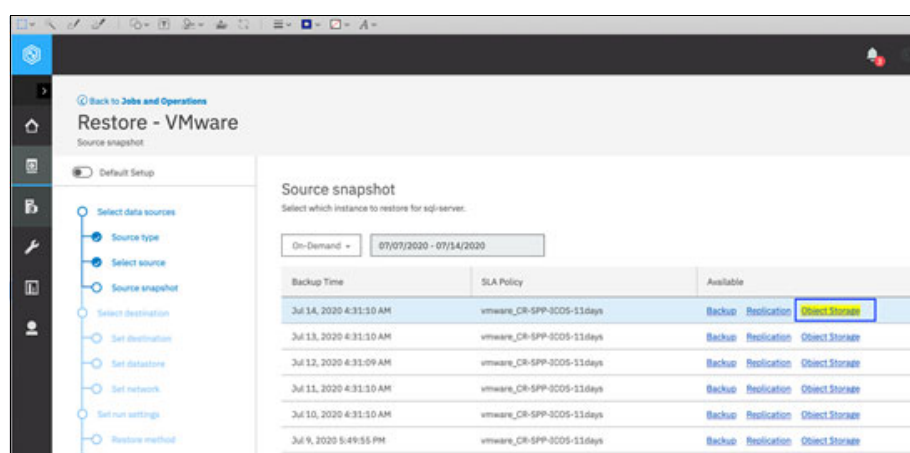


Figure 27 Selecting restore operation from WORM copies of IBM Cloud Object Storage

4. Select the destination to restore non-tampered copies from IBM Cloud Object Storage. In our example, we restore the copy at IBM Cloud location by selecting the **Alternate Host or Cluster** option. Select the ESXi server location in IBM Cloud. Select the **Use alternative vSnap server for the restore job** option and then, select the **Remote vSnap server** from the alternative vSnap server drop-down list. Then, click **Next** (see Figure 28 on page 26).

When you restore data from a restore point that was copied to a cloud resource or repository server, a vSnap server is used as a gateway to complete the operation.

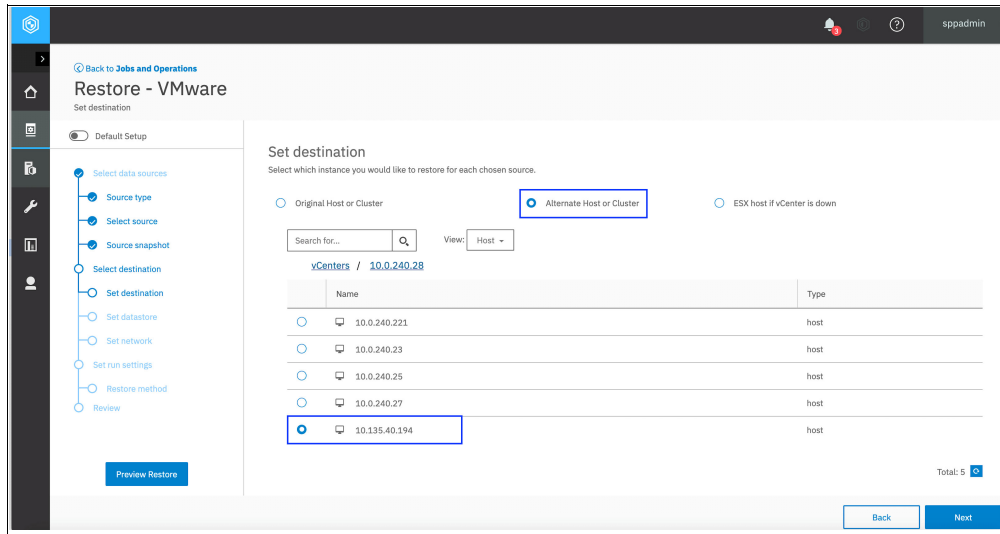


Figure 28 Selecting location to restore IBM Cloud Object Storage WORM copies

- Set datastore and Set network options as needed. In Set network options, you can map and provide the network information at the IBM Cloud site to set up networking on the virtual machine during restore process.
- In Set run settings and under Restore method, select the restore method to be used for the source selections. For our example, we validated with both Test and Clone methods to restore non-tampered copies from the IBM Cloud Object Storage. Enter the name of the virtual machine to be restored at the IBM Cloud location (see Figure 29).

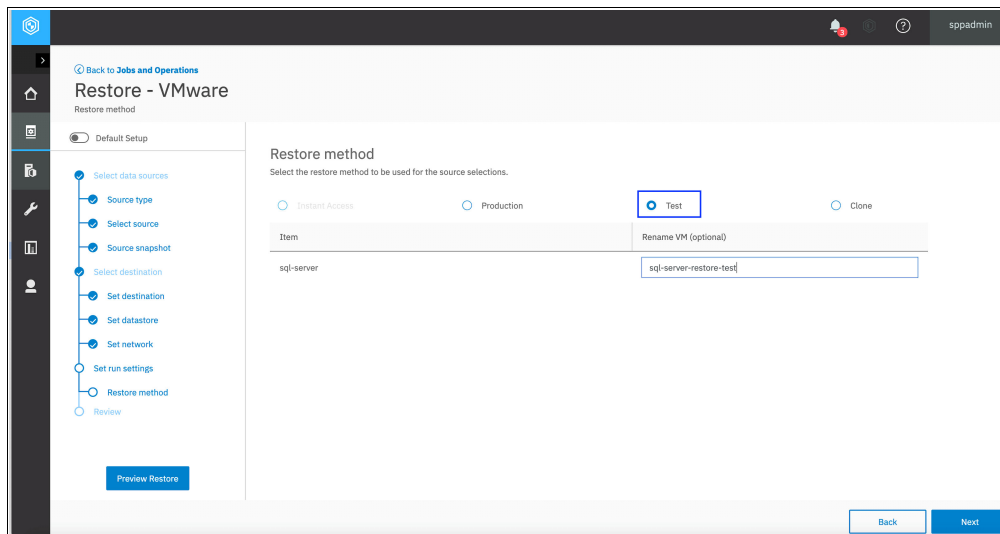


Figure 29 Selecting type of restore at IBM Cloud location

- Review the restore settings and click **Submit** to start restore job. Validate the restore job by browsing to Jobs and Operations and Running Jobs tab.

This restored virtual machine from WORM buckets of IBM Cloud Object Storage provides non-tampered copies of protected data.

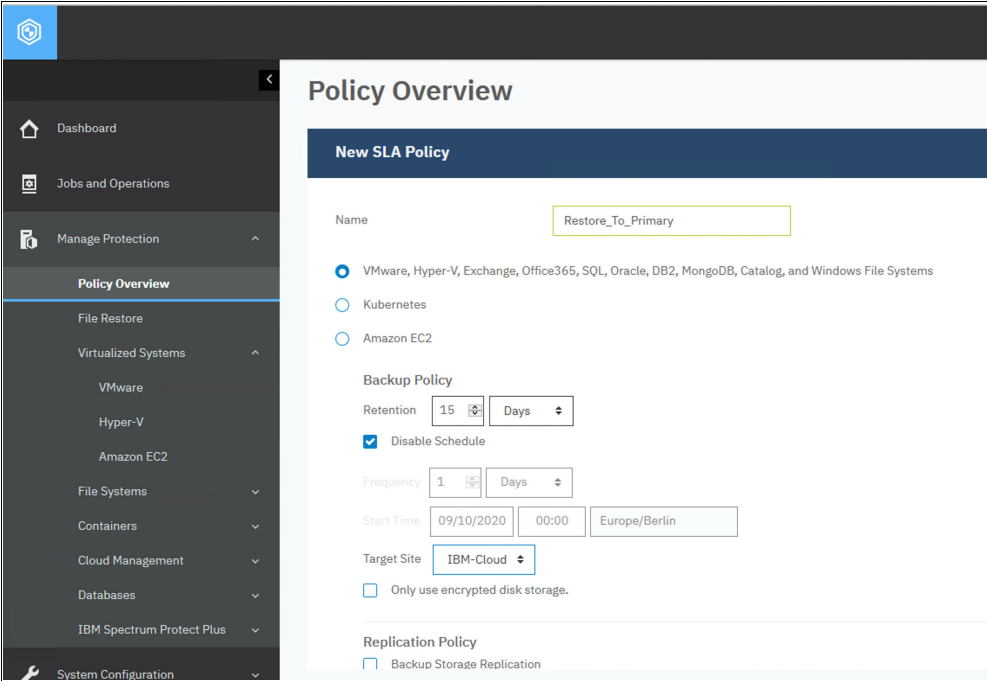
Restoring virtual machines to the primary site

After the non-tampered copy of data is located and restored from IBM Cloud Object Storage on IBM Cloud site, it must be restored to production. In addition to other methods of restoring or replicating virtual machines to primary site, IBM Spectrum Protect Plus can be used to restore virtual machines to primary site.

In this section, we demonstrate restoring the non-corrupted copy back to primary site by using IBM Spectrum Protect Plus. Complete the following steps:

1. The first restored machine in IBM Cloud must be registered in IBM Spectrum Protect Plus. To register non-corrupted copy that is restored from IBM Cloud Object Storage, select **Manage Protection** → **VMware** → **Run Inventory** on the vCenter server to register it in IBM Spectrum Protect Plus.
2. Create an SLA policy in IBM Spectrum Protect Plus to restore the copy to the primary site. In a new SLA policy, back up the restored virtual machine to IBM Cloud and then, replicate it to the primary site.

Select **Manage Protection** → **Policy Overview** → **Add SLA Policy** and enter the name for the new SLA Policy and select the first option of backing up VMware virtual machine. For this policy, we select **Disable Schedule**. Select **Target Site** for backup as remote vSnap server first (see Figure 30).



The screenshot displays the 'Policy Overview' page in the IBM Spectrum Protect Plus interface. On the left is a dark sidebar with navigation options: Dashboard, Jobs and Operations, Manage Protection (expanded), Policy Overview (selected), File Restore, Virtualized Systems (expanded), VMware, Hyper-V, Amazon EC2, File Systems, Containers, Cloud Management, Databases, IBM Spectrum Protect Plus, and System Configuration. The main content area is titled 'Policy Overview' and contains a 'New SLA Policy' form. The form fields are: Name (Restore_To_Primary), Backup Policy (VMware, Hyper-V, Exchange, Office365, SQL, Oracle, DB2, MongoDB, Catalog, and Windows File Systems selected), Retention (15 Days), Backup Policy (checked), Disable Schedule (checked), Frequency (1 Days), Start Time (09/10/2020 00:00 Europe/Berlin), Target Site (IBM-Cloud), Only use encrypted disk storage (unchecked), and Replication Policy (Backup Storage Replication unchecked).

Figure 30 Selecting type of restore at IBM Cloud location

3. In the Replication Policy section, select the **Backup Storage Replication** → **Disable Schedule** → **Same as source selection** options. Click **Save** (see Figure 31 on page 28).

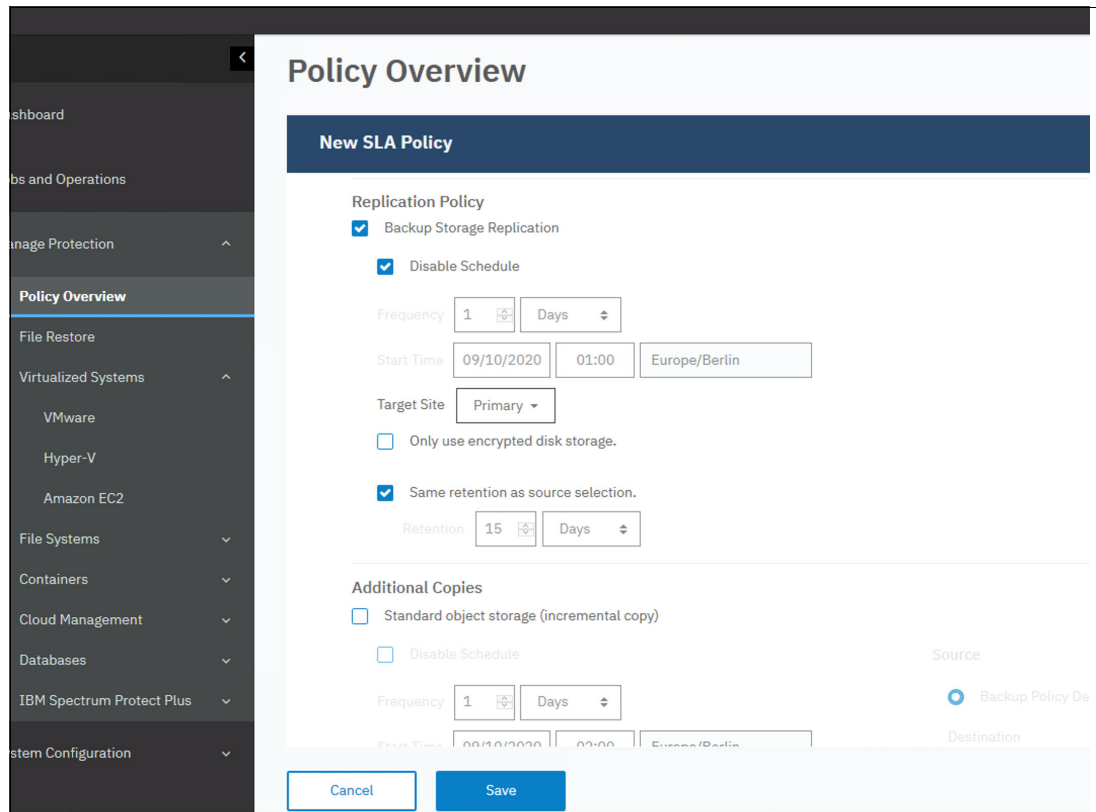


Figure 31 Select replication options in SLA policy to bring restored data to primary

4. To start backing up the non-corrupted restored virtual machine from IBM Cloud Object Storage WORM bucket to the remote vSnap server, select **Manage Protection** → **Virtualized Systems** and the selected VMware. Then, browse to the vCenter server and then select the virtual machine in the SLA Policy tab. In the SLA policies, select the SLA policy that was created in Step 2 (see Figure 32).

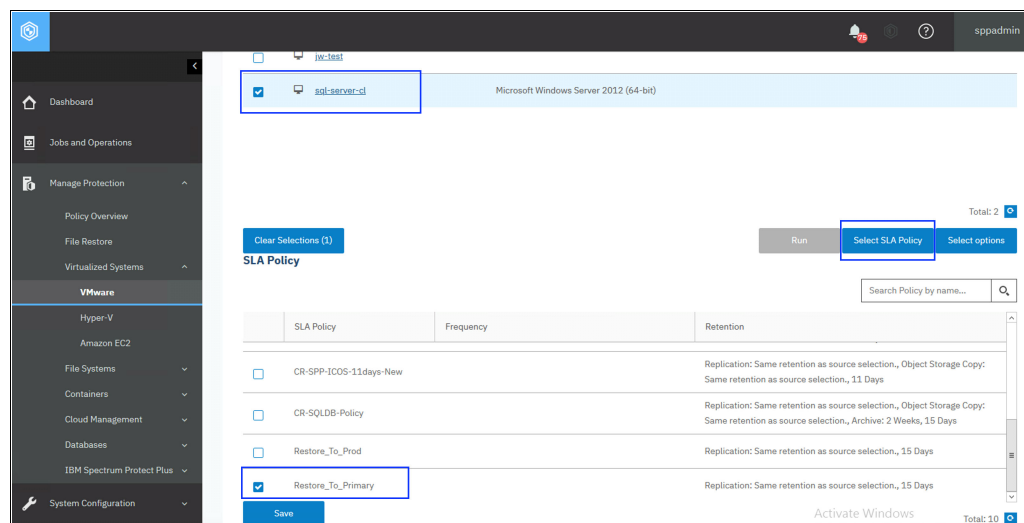


Figure 32 Starting backup to remote vSnap using SLA policy

5. Select the newly created SLA Policy and then, with the virtual machine selected, click **Actions** → **Start**. In the Start Options, select **SLA Policy** as Backup to vSnap in the drop-down list and click **OK** to start the backup (see Figure 33).

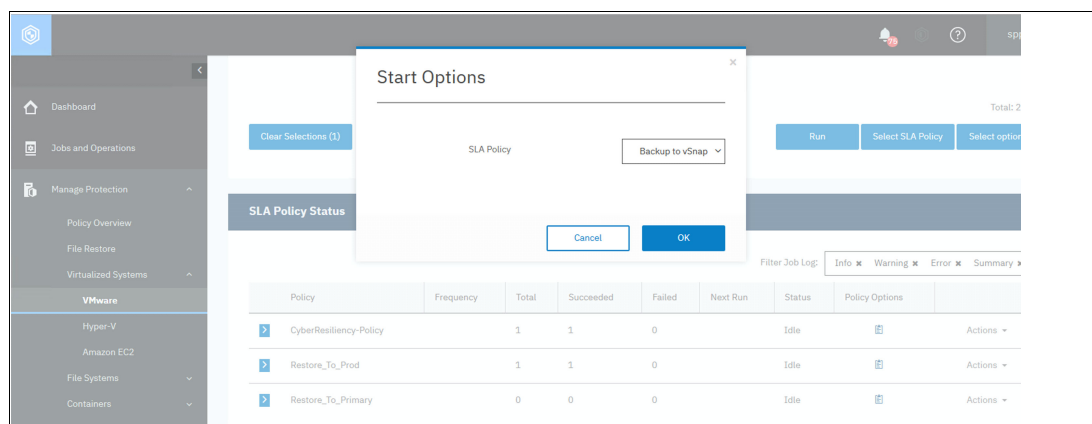


Figure 33 Selecting backup to remote vSnap from SLA policy

6. Monitor the backup job in Jobs and Operations. After the backup is successful, replicate the backed up virtual machine data from the IBM Cloud vSnap server to the vSnap server at the primary site.

For starting replication, select **Manage Protection** → **Virtualized Systems** and then the selected VMware. Then, browse to the vCenter server and select the virtual machine. Select the **SLA Policy** tab. In the SLA policies, select newly created SLA policy. Click **Actions** → **Start**. In the Start Options, select SLA Policy as **Replicate** in a drop-down menu and click **OK** to start replication (see Figure 34).

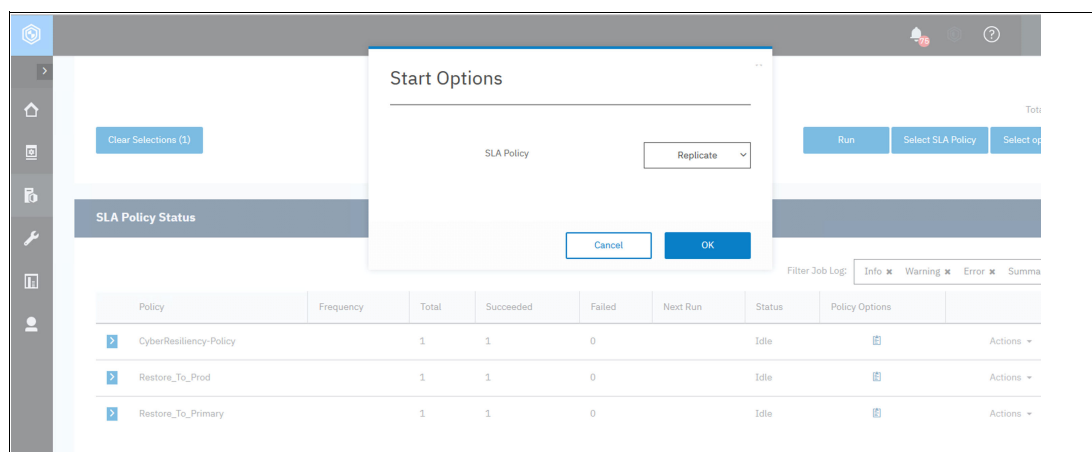


Figure 34 Starting replication job from remote vSnap to primary site

7. Monitor the replication job in Jobs and Operations and in the Running Jobs tab.
8. After successful replication to the vSnap server on primary, virtual machine data can be restored on the primary site (see Figure 35). Complete the following steps to restore the replicated virtual machine:
 - a. Start a restore job.
 - b. Select the source of the virtual machine from IBM Cloud location.
 - c. In Source snapshot, select **Replication snapshot** to be restored from data that is replicated to the primary site vSnap server.

- d. Select **Alternative ESXi server** to which to restore. In this case, select **ESXi server** on the primary site. Then, select the data store and the suitable networking options on the primary site and start restoring the data to the primary site (see Figure 35).

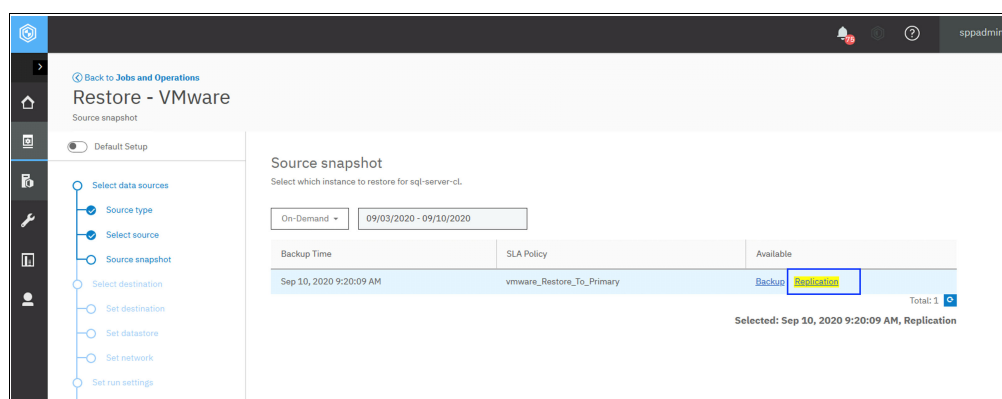


Figure 35 Selecting restore option to restore data back to primary

SQL Server data backup to IBM Cloud Object Storage WORM buckets

IBM Spectrum Protect Plus facilitates backing up applications and databases, such as Oracle databases or SQL databases. For more information about the prerequisites and requirements before backing up SQL database to IBM Spectrum Protect Plus, see [IBM Knowledge Center](#) and search for “Protecting Databases and SQL Server”.

In this publication, we demonstrate backing up an SQL Server database instance to IBM Cloud Object Storage WORM buckets to protect it from cyber events and restore non-tampered copies from IBM Cloud Object Storage WORM instance inside the IBM Cloud location. This process demonstrates that applications that are supported through IBM Spectrum Protect Plus can also be protected against cyber events by storing the copies to IBM Cloud Object Storage WORM buckets.

Backing up SQL databases to IBM Cloud Object Storage WORM buckets follows the same flow as explained in “Protecting virtual machine data to IBM Cloud Object Storage WORM buckets” on page 21. First, it is backed up to the vSnap server at primary site and then, it is replicated to the remote vSnap server. Then, replicated copies of SQL database are copied to IBM Cloud Object Storage WORM buckets in IBM Cloud.

Complete the following steps:

1. To back up SQL databases in IBM Spectrum Protect Plus, the SQL database application must be registered in IBM Spectrum Protect Plus:
 - a. Select **Manage Protection** → **Databases** → **SQL**.
 - b. Select **Manage Application servers** and click **Add application server**.
 - c. Enter the details of SQL server instance at IBM Cloud to save and register the SQL server instance in IBM Spectrum Protect Plus.
2. Create an SLA policy to back up to primary vSnap server, replicate to remote vSnap server, and copy the SQL database backup to IBM Cloud Object Storage WORM buckets inside IBM Cloud as explained in “Copying protected data from remote vSnap server to IBM Cloud Object Storage WORM buckets” on page 23.

3. To back up an SQL database to the primary vSnap server (see Figure 36):
 - a. Select **Manage Protection** → **Databases** → **SQL**.
 - b. Browse to the SQL server instance in SQL Backup and select the SQL database instance that must be backed up.
 - c. Select the newly created SLA Policy and select **Actions** → **Start**.
 - d. Select **Backup to vSnap** from drop-down SLA Policy list in the Start Options window.
 - e. Click **OK** to start the backup to vSnap server at primary site. Monitor the backup and verify that the backup to vSnap server at primary site was successful.

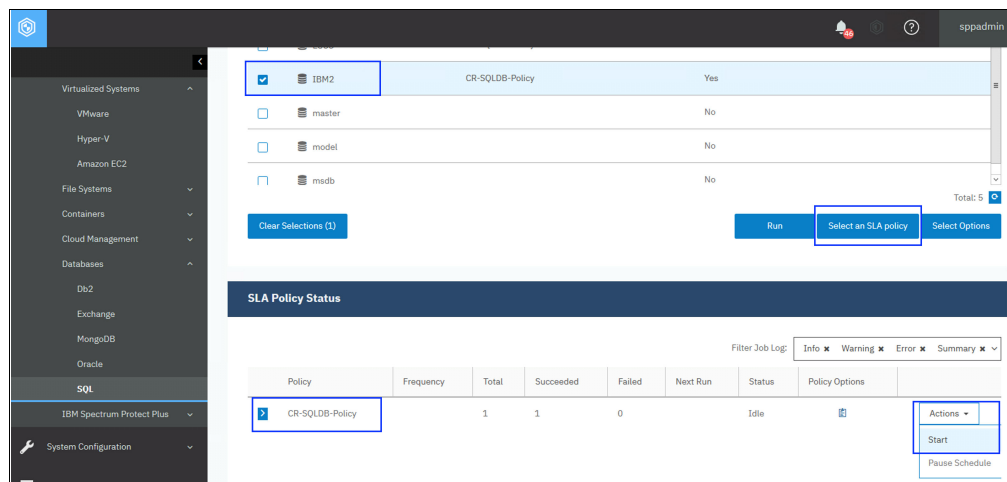


Figure 36 Starting SQL Server database backup to primary vSnap server

4. After the back up to vSnap server at primary site is successful, repeat the same procedure and select **Replication** from drop-down SLA Policy list in Start Options window. Then, click **OK** to start replication to the vSnap server at the remote site. Monitor the replication job and verify that the replication to the remote vSnap server was successful (see Figure 37).

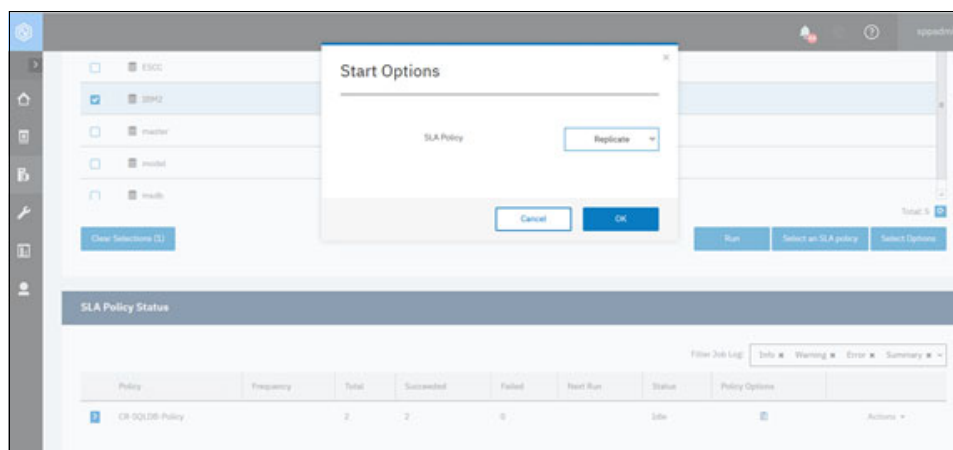


Figure 37 Replicating SQL server back up to remote vSnap server

5. After the successful replication to the remote vSnap server, the SQL database data can be copied to IBM Cloud Object Storage immutable WORM buckets in IBM Cloud (see Figure 38). After data is copied inside WORM buckets of IBM Cloud Object Storage, it cannot be overwritten, deleted, or tampered with, which protects it from cyber-events.

For copying data from a remote vSnap server to IBM Cloud Object Storage WORM buckets, repeat the same procedure step 3 and select **Copy** from drop-down SLA Policy list in Start Options window. Then, click **OK** to start copying the data to IBM Cloud Object Storage WORM bucket. Monitor the copy job and verify that the copy to IBM Cloud Object Storage WORM bucket was successful (see Figure 38).

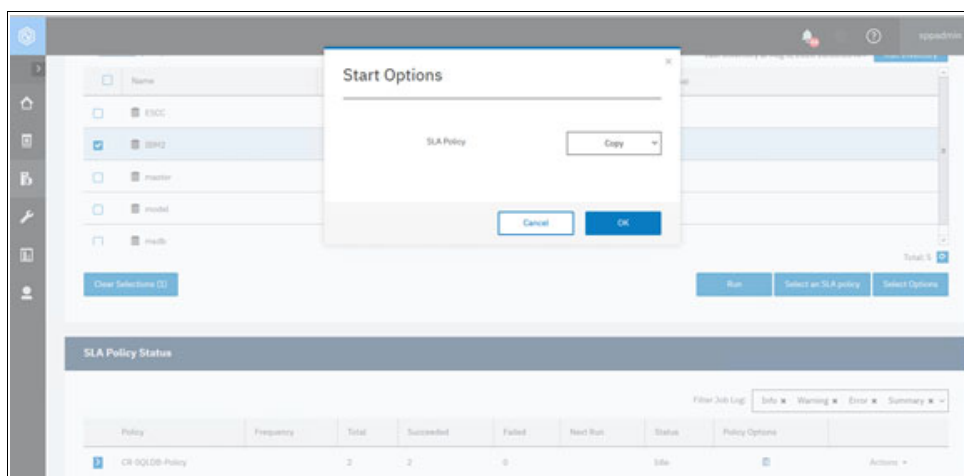


Figure 38 Starting SQL server backup copy to IBM Cloud Object Storage WORM buckets

Recovering SQL Server data from IBM Cloud Object Storage

Backed up SQL databases can be restored and recovered from IBM Cloud Object Storage WORM buckets in IBM Cloud. In a normal restore scenario, SQL databases can be directly restored from the primary vSnap server or remote vSnap server.

After the cyber events occur, it is important to know when the event occurred and then recover the non-corrupted copies of database before the cyber events.

For more information and prerequisites, see [IBM Knowledge Center](#) and search for “Restoring SQL Server data”.

Complete the following steps:

1. To restore or verify non-corrupted copies of data in IBM Cloud location, select **Jobs and Operations** → **Create Job** → **Restore** and then, the source type as **SQL** in the Databases section. Browse the SQL server database to recover and then select **Database instance to recover**.
2. Select the **On-demand: Snapshot restore** and then, select **Object Storage** as the source snapshot (see Figure 39 on page 33). This selection ensures that the SQL database instance is recovered from IBM Cloud Object Storage WORM buckets.

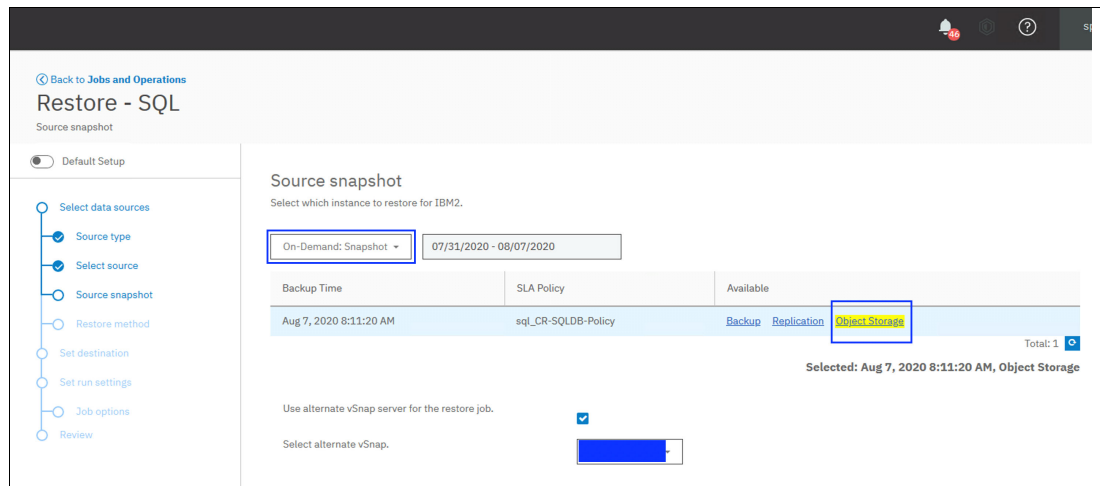


Figure 39 Restoring SQL server copy from IBM Cloud Object Storage WORM buckets

3. After selecting snapshot from Object Storage to be recovered, select the nearest vSnap server. In this case, select **Select alternative vSnap** → **Remote vSnap server**. The SQL database is recovered from where the protected data is copied to the IBM Cloud Object Storage WORM buckets.

Note: When you restore data from a restore point that was copied to a cloud resource or repository server, a vSnap server is used as a gateway to complete the operation.

4. In the next window, select the restore method to be used for source selections: Instance access, Production, or Test. Select the **New Database Name** option for the restored database instance and Destination Path (see Figure 40).

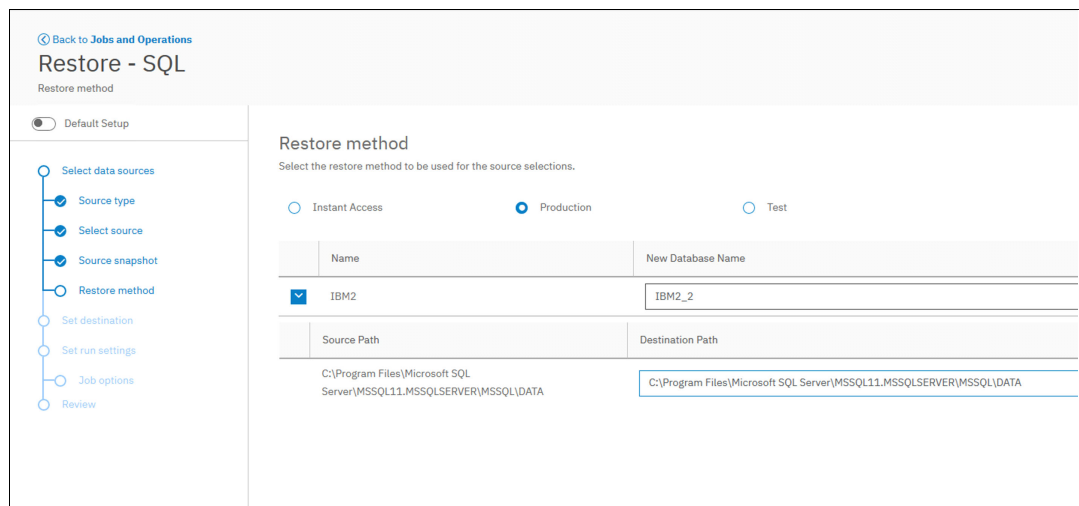


Figure 40 Selecting SQL server restore options

5. In the Set destination window, select the instance to where you want to restore each selected source. In our example, select **IBM Cloud location** and then, select the server instance (see Figure 41).

[Back to Jobs and Operations](#)

Restore - SQL

Set destination

☐ Default Setup

- Select data sources
- Source type
- Select source
- Source snapshot
- Restore method
- Set destination**
- Set run settings
- Job options
- Review

Set destination

Select which instance you would like to restore for each chosen source.

☐ Restore to original instance ☒ Restore to alternate instance

Search for instance...

[Instances](#)

	Name	Version
<input type="radio"/>	SQL-SERVER	11.0.3000.0
<input checked="" type="radio"/>	SQL-SERVER-CLON	11.0.3000.0

Figure 41 Selecting SQL server restore destination to IBM Cloud

6. Select the Job options, review the restore settings, and click **Submit** to start the restoration of the SQL server database instance from IBM Cloud Object Storage WORM buckets. Monitor the restore job by selecting **Jobs and Operations** → **Running Jobs** tab. Verify the restored SQL server database instance. This restored SQL server database instance from the WORM buckets of IBM Cloud Object Storage provides non-tampered copies of protected SQL server database data.
7. Repeat the same procedure to bring the validated and non-corrupted copy of database instance to the primary site per the use case of Restore back virtual machine to the Primary Site. Select SQL Server data backup and restore operations instead of virtual machine backup and restore operations (see “Restoring virtual machines to the primary site” on page 27).

Backing up and recovering the IBM Spectrum Protect Plus server

As part of core infrastructure, IBM Spectrum Protect Plus server can also be the target of cyber attacks. IBM Spectrum Protect Plus server’s internal database and configuration can be backed up, replicated, and copied to IBM Cloud Object Storage’s WORM buckets. If a cyber event or attack on IBM Spectrum Protect Plus server occurs, it can be restored from the non-tampered copies that are inside IBM Cloud Object Storage if a complete loss of backup infrastructure and configuration occurs. For more information, see [IBM Knowledge Center](#) and search for “Protecting IBM Spectrum Protect Plus”.

Conclusion

Cyber attacks are likely to remain risk for the foreseeable future. Attacks on the organizations can be external and internal. Investing in technology and processes to prevent these cyber attacks is the highest priority for the organizations.

Organizations need well-designed procedures and processes to recover from the eventful attacks. Adoption of the NIST framework, the proper discipline of risk management, and IBM Storage's offerings can be used to create and implement recovery plans that assure the safety of business-critical data.

IBM Spectrum Protect Plus is a modern data protection solution that provides near-instant recovery, replication, reuse, and self-service for virtual machines, databases, and applications in hybrid cloud environments. IBM Cloud Object Storage is an unstructured data storage service that is designed for durability, resilience, and security.

IBM Spectrum Protect Plus' capability to copy the protected data to IBM Cloud Object Storage WORM buckets based on retention policies allows organizations to implement easy to manage and automate cyber resilience solution across hybrid cloud. These solutions provide robust protection external cyber events, such as malware, ransomware attacks, internal cyber events.

Also, IBM Spectrum Protect Plus can offload the protected data to tape store by way of IBM Spectrum Protect for achieving long-term retention and air-gapping by storing the tapes off-site. It can create ultimate protection against external and internal cyber events.

The configuration and examples of operations that are described in this document are for illustration purpose only. The real-world implementation of hybrid cloud setup, the configuration of IBM Spectrum Protect Plus supported storage system, VMware environment, IBM Spectrum Protect Plus, and IBM Cloud Object Storage in IBM Cloud, setting up policies, and execution of operations can vary per network bandwidth for achieving better scalability and performance and ultimately achieving cyber resilience.

Related resources

The following resources provide more information about the topics that are discussed in this Blueprint:

- National Institute of Standards and Technology Cyber Security Framework:
<https://www.nist.gov/cyberframework>
- IBM Spectrum Protect Plus (IBM Knowledge Center):
https://www.ibm.com/support/knowledgecenter/SSNQFQ_10.1.6/spp/welcome.html
- IBM Cloud Object Storage (IBM Knowledge Center):
https://www.ibm.com/support/knowledgecenter/en/STXNRM_3.15.1/coss.doc/kc_welcome.html?pos=2
- Getting started with IBM Cloud Object Storage on IBM Cloud:
<https://cloud.ibm.com/docs/cloud-object-storage?topic=cloud-object-storage-getting-started-cloud-object-storage>

- IBM FlashSystem (IBM Knowledge Center):
https://www.ibm.com/support/knowledgecenter/en/STSLR9_8.3.1/com.ibm.fs9200_831.doc/fs9200_ichome.html
- Getting started with IBM Cloud Virtual Private Networking:
<https://cloud.ibm.com/docs/iaas-vpn?topic=iaas-vpn-getting-started>
- VMware vSphere documentation:
<https://docs.vmware.com/en/VMware-vSphere/index.html>

About the author

Mandar J. Vaidya is storage solutions architect with IBM Storage. Mandar has over 20 years of experience working in storage and systems. Mandar has created various storage solution with various IBM Storage offerings and IBM's technology partners and published solution papers. Mandar is currently working on designing cybersecurity and cyber resilience solutions with IBM Storage offerings. Mandar holds a Bachelor of Engineering degree from the University of Pune, India.

Acknowledgments

The author would like to acknowledge Joerg Walter for his expertise and assistance in setting up hybrid cloud environment between IBM lab and IBM Cloud.

Author would also like to acknowledge Julio Hernandez, WW Offering Manager for Storage Cyber Resilience, for his guidance and assistance during the creation of this proof of concept and solution paper.

Notices

This information was developed for products and services offered in the US. This material might be available from IBM in other languages. However, you may be required to own a copy of the product or product version in that language in order to access it.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing, IBM Corporation, North Castle Drive, MD-NC119, Armonk, NY 10504-1785, US

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

IBM may use or distribute any of the information you provide in any way it believes appropriate without incurring any obligation to you.

The performance data and client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

Statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to actual people or business enterprises is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at “Copyright and trademark information” at <http://www.ibm.com/legal/copytrade.shtml>

The following terms are trademarks or registered trademarks of International Business Machines Corporation, and might also be trademarks or registered trademarks in other countries.

Aspera®


IBM®

IBM Cloud®

IBM FlashCore®

IBM FlashSystem®

IBM Spectrum®

Redbooks (logo) ®

Storwize®

The following terms are trademarks of other companies:

The registered trademark Linux® is used pursuant to a sublicense from the Linux Foundation, the exclusive licensee of Linus Torvalds, owner of the mark on a worldwide basis.

Microsoft, Windows, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

VMware, VMware vCenter Server, VMware vSphere, and the VMware logo are registered trademarks or trademarks of VMware, Inc. or its subsidiaries in the United States and/or other jurisdictions.

Other company, product, or service names may be trademarks or service marks of others.

Terms and conditions for product documentation

Permissions for the use of these publications are granted subject to the following terms and conditions.

Applicability

These terms and conditions are in addition to any terms of use for the IBM website.

Commercial use

You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of IBM.

Rights

Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

IBM reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by IBM, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

IBM MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.

Privacy policy considerations

IBM Software products, including software as a service solutions, ("Software Offerings") may use cookies or other technologies to collect product usage information, to help improve the end user experience, to tailor interactions with the end user, or for other purposes. In many cases no personally identifiable information is collected by the Software Offerings. Some of our Software Offerings can help enable you to collect personally identifiable information. If this Software Offering uses cookies to collect personally identifiable information, specific information about this offering's use of cookies is set forth below.

This Software Offering does not use cookies or other technologies to collect personally identifiable information.

If the configurations deployed for this Software Offering provide you as customer the ability to collect personally identifiable information from end users via cookies and other technologies, you should seek your own legal advice about any laws applicable to such data collection, including any requirements for notice and consent.

For more information about the use of various technologies, including cookies, for these purposes, see IBM's Privacy Policy at <http://www.ibm.com/privacy> and IBM's Online Privacy Statement at <http://www.ibm.com/privacy/details> in the section entitled "Cookies, Web Beacons and Other Technologies," and the "IBM Software Products and Software-as-a-Service Privacy Statement" at <http://www.ibm.com/software/info/product-privacy>.



© Copyright IBM Corporation

November 2020

US Government Users Restricted Rights - Use, duplication or disclosure restricted by GSA ADP Schedule
Contract with IBM Corp.



Please recycle

ISBN 0738459186

REDP-5624-00