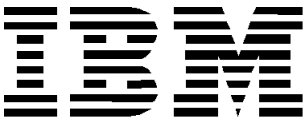
IBM® Storage

A Hybrid Cloud Cyber Security Solution using IBM Spectrum Virtualize for Public Cloud on Azure and IBM Spectrum Virtualize Safeguarded Copy



Contents

About this document

The document describes the configuration and end-to-end architecture for configuring the logical air-gap solution for cyber resiliency using IBM® Spectrum Virtualize for Public Cloud (SV4PC) on Azure, IBM Spectrum® Virtualize Safeguarded Copy, and IBM FlashSystem®.

Important: 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 Spectrum Virtualize for Public Cloud on Azure and IBM FlashSystem are supported and entitled and where the issues are specific to a blueprint implementation.

Executive summary

In today's world, data security is of utmost importance. Data can be compromised by human error, system glitches, or malicious criminal acts.

Data breaches are among the gravest and most expensive threats to businesses today.

The traditional business continuity solutions most organizations developed and implemented use high availability (HA) and disaster recovery (DR) to protect their data. However, these solutions alone are not sufficient enough to protect against the cyberattacks.

According to the 2020 Cost of Data Breach Report, the average cost worldwide of a data breach in the preceding 12 months was $4 million, which is an adjusted average total cost. In addition to loss of revenue, organizations that are affected by a breach run the risk of having their normal business operations disrupted, and losing valuable data, customers, and reputation within their industry.

Cyber resilience solutions are developed by organizations to continue operating with the least amount of disruption despite cyberattacks and outages. Cyber resilience expands the scope of protection, covering cybersecurity and business continuity.

A significant part of cyber resilience is the ability to recover from a logical data corruption event. Because this unrelenting tide of data breaches is driving increased interest in providing assured data integrity across hybrid cloud environments, IBM Spectrum Virtualize offers the powerful data security function of IBM Safeguarded Copy.

IBM Spectrum Virtualize for Public Cloud is a software-defined storage solution that supports many features that are included as part of IBM FlashSystem storage products that run IBM Spectrum Virtualize software. IBM Spectrum Virtualize for Public Cloud supports various cloud-based use cases, such as all-in cloud, cloud-to-cloud, and hybrid-cloud deployments.

IBM Spectrum Virtualize for Public Cloud software can be deployed in Microsoft Azure. The IBM Spectrum Virtualize for Public Cloud installation is offered through the Azure Marketplace as a Bring Your Own license (BYOL) solution.

During installation, the IBM Spectrum Virtualize for Public Cloud deployment is implemented through an Azure Managed Resource (ARM) template that gathers parameters and credentials from the user, verifies entitlement, and creates all Azure resources that are required to deploy IBM Spectrum Virtualize for Public Cloud instance in Microsoft Azure.

Scope

This blueprint guide provides the following information:

- A solutions architecture and related solution configuration workflows, with the following essential software and hardware components:
  - IBM FlashSystem
  - IBM Spectrum Virtualize for Public Cloud on Azure
  - IBM Copy Services Manager
- Detailed technical configuration steps for building the cyber resiliency solutions

This technical report does not provide performance analysis from a user perspective or replace any official IBM manuals or documents.

Prerequisites

This technical paper assumes that the reader is familiar with the following areas:

- Basic knowledge of IBM FlashSystem
- Azure Cloud fundamentals
- Hybrid Cloud network connectivity
- IBM Copy Services Manager

Blueprint roadmap

This blueprint includes the following topics:

- The basic components of the IBM Spectrum Virtualize Safeguarded Copy are demonstrated in a single site configuration.
- The solution is expanded to illustrate an airgap configuration in which a second site is introduced and replication is configured between the sites. Then, the Safeguarded Copy is taken at the second site to provide physical isolation.
- At the end of the document the similarity of an on-premises to Azure airgap solution is discussed. The only difference is the necessity for setting up the site-to-site VPN tunnel to facilitate the IBM Spectrum Virtualize replication from on-premises to Azure.

Getting Started: Cyber Security Solution that uses Safeguarded Copy in IBM Spectrum Virtualized for Public Cloud in Azure

This section describes the essential building blocks for creating the logical airgap, cyber resiliency solution that uses the Safeguarded Copy feature that is available in IBM FlashSystem with IBM Spectrum Virtualize.

IBM FlashSystem family

IBM FlashSystem Family is an excellent platform to simplify your hybrid multicloud storage.

The new IBM FlashSystem family, along with IBM Spectrum Virtualize for Public Cloud, simplifies storage for hybrid cloud environments. With a unified set of software, tools, and APIs, IBM FlashSystem addresses the entire range of storage needs, all from one data platform that extends enterprise functions across the storage system.

IBM Spectrum Virtualize

With IBM Spectrum Virtualize software, the IBM FlashSystem family is an industry-leading storage solution that includes technologies that complement and enhance virtual environments to achieve a simpler, more scalable, and cost-efficient IT infrastructure.

To further drive your IT transformation, IBM Spectrum Virtualize for Public Cloud offers multiple ways to create hybrid cloud solutions between on-premises private clouds and the public cloud. It enables real-time storage-based data replication and disaster recovery, and data migration between local storage and AWS, IBM Cloud®, or Microsoft Azure. This feature enables storage administration at a cloud service provider's site in the same way as on-premises, regardless of the type of storage.

For more information about IBM FlashSystem, see this web page.

IBM FlashSystem storage solutions include the following features:

- NVMe-accelerated flash arrays with control enclosures that are end-to-end NVMe-enabled, with flexibility to choose and mix between IBM FlashCore® Modules, industry standard NVMe drives and Storage-Class Memory. The systems offer industry-leading performance and scalability with support for bare-metal, virtual, and containerized environments.
- Built with IBM Spectrum Virtualize, with a full range of industry-leading data services, such as dynamic tiering, IBM FlashCopy® management, data mobility, and high-performance data encryption.
- Hybrid cloud ready, with support for private, hybrid, or public cloud deployments. The solutions come with ready-to-use, proven, validated "cloud blueprints" with support for cloud API automation and secondary data orchestration software.
- Cost-efficient, with innovative data reduction pool (DRP) technology that includes deduplication and hardware-accelerated compression technology, plus SCSI UNMAP support and all the thin provisioning, copy management, and efficiency you expect from IBM Spectrum Virtualize based storage.
- Hybrid storage enabled, with multiple expansion enclosure options that are based on 12 Gbps SAS that support solid-state drives (SSDs) and hard disk drives (HDDs).

- IBM FlashSystem®, which is ready for new generation applications that support Red Hat OpenShift, Container Storage Interface (CSI), Ansible automation, and Kubernetes, along with traditional VMWare and bare-metal environments.
- IBM Cloud Satellite™, which helps you deploy consistently across all on-premises, edge computing and public cloud environments from any cloud vendor. The result is greater developer productivity and development velocity. The IBM FlashSystem family is the perfect storage choice for IBM Cloud Satellite because of its simplicity, high performance, and low latency.
- IBM Copy Services Manager coordinates and automates Safeguarded Copy function across multiple systems
- IBM Spectrum Virtualize for Public Cloud can be deployed in a Microsoft Azure for various cloud-based uses cases, such as including all-in-cloud, cloud-to-cloud, and hybrid-cloud deployments.
- The IBM Spectrum Virtualize for Public Cloud installation is offered through Azure Marketplace as a Bring Your Own License (BYOL). During installation, the IBM Spectrum Virtualize for Public Cloud deployment template gathers deployment parameters from user, verifies your license, and creates all Azure resources that are required to deploy your IBM Spectrum Virtualize for Public Cloud instance in Microsoft Azure.

Lab setup

Figure 1 shows the architecture that was deployed in our lab to show the IBM Safeguarded Copy setup for cyber resiliency solution for volumes in SV4PC in Azure.

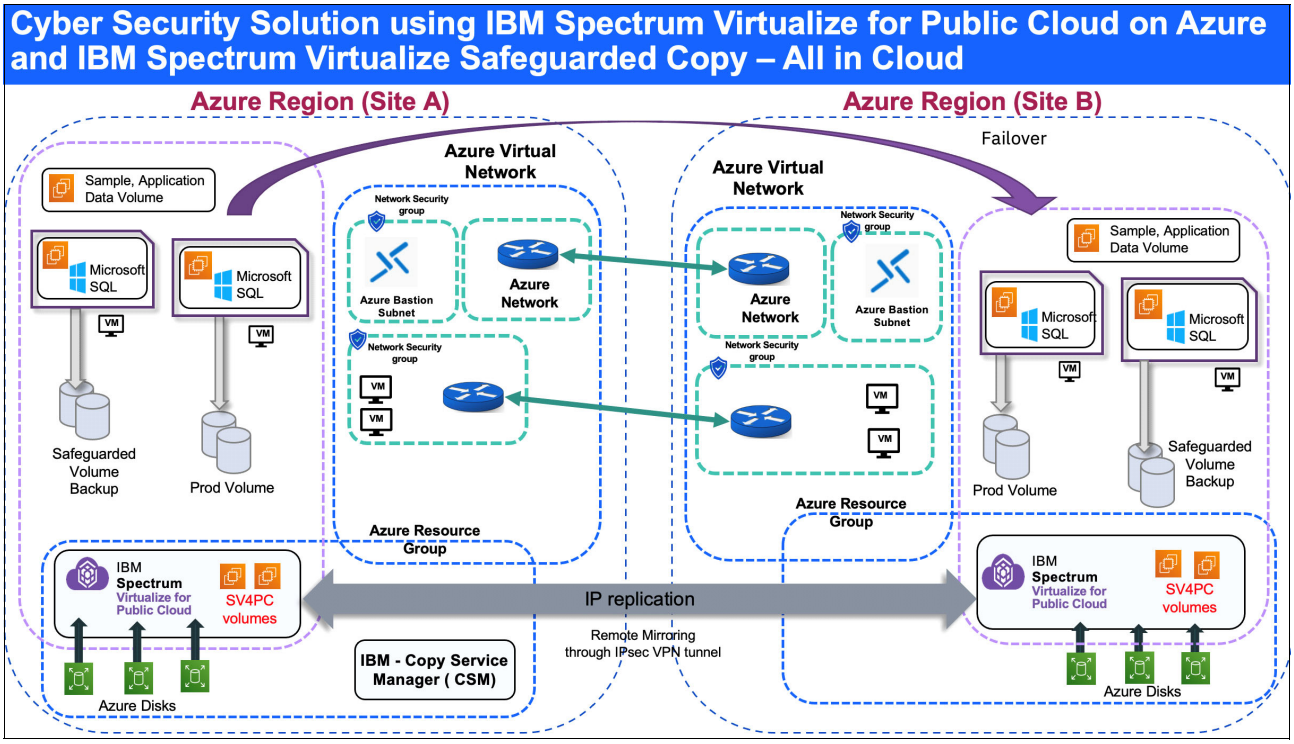


Figure 1 Lab setup cybersecurity solution

In this sample configuration, IBM Spectrum Virtualize for Public Cloud in Azure is used as an all-in-cloud scenario to demonstrate the cyber resiliency solution by using the IBM Spectrum Virtualize for Public Cloud Safeguarded Copy feature.

Note: The terms *Site A* and *Site B* are applied for the Azure region for the purpose of this publication. In reality, Site A and Site B do not exist in Azure.

Next, we describe the steps that were used in th the lab configuration to demonstrate the solution.

The single site scenario included the following steps:

1. Deployed IBM Spectrum Virtualize for Public Cloud (SV4PC) in Azure.
2. Created a Safeguarded Pool on IBM Spectrum Virtualize for Public Cloud in Azure.
3. Set up a volume group and added volumes to it.
4. Reviewed the predefined Safeguarded policies (frequency and retention of backups).
5. Associated a predefined policy or created a policy by using the command-line interface (CLI) and associated it with the volume group.
6. Installed and configured the IBM Copy Services Manager with IBM Spectrum Virtualize.

   The crash consistent Safeguarded backup of production volumes in IBM Spectrum Virtualize for Public Cloud in Azure is taken automatically by IBM Copy Services Manager according to the associated policy.
7. Restored (to the original volume) or recovered (to a new volume) data from immutable safeguarded backups.
8. Restored from a Safeguarded backup.

For the airgap scenario, we replicated the IBM Spectrum Virtualize for Public Cloud storage volume between two sites in Azure

Single-site scenario: Deploy IBM Spectrum Virtualize for Public Cloud in Azure

For this scenario, it is assumed that IBM Spectrum Virtualize for Public Cloud (SV4PC) is deployed on Azure. For more information about deployment instructions, see this IBM Documentation web page.

Post deployment of SV4PC on Azure, virtual machines (VMs) are deployed in the lab setup. Also, we created two other hosts (`Restore-VM-Hemanand`, and `VM-Hemanand`) to assign iSCSI volumes to these hosts from SV4PC storage for the demonstration, as described next.

The following VMs that are in Azure are shown in Figure 2:

- Windows Server 2019 VM: `Restore-VM-Hemanand`
- SV4PC node 1: `sv-Hemanand-node1-vm`
- SV4PC node 2: `sv-Hemanand-node2-vm`
- SV4PC quorum node: `sv-Hemanand-quorum`
- Windows Server 2019 VM: `VM-Hemanand`

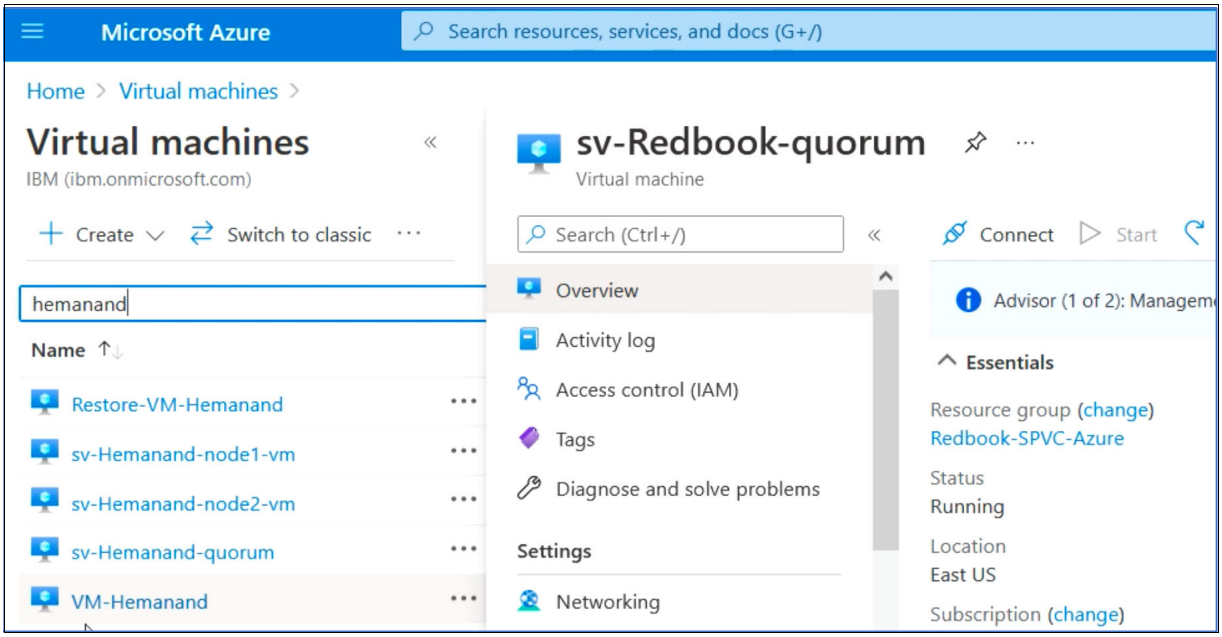


Figure 2 Azure virtual resource in resource group

Complete the following steps:

1. Post deployment of SV4PC on Azure, log in to the SV4PC Cluster by using the Bastion Service on Azure, or log in to the SV4PC Cluster by using the Windows VM that was created in Azure with access to the SV4PC cluster.

   In this demonstration, we logged in to the SV4PC Cluster by using the Windows VM.

2. Log in to the `VM-hemanand` host (Windows 2019 server) with RDP and open the SV4PC cluster IP URL from a web browser: `https://40.10.1.28:8443/login`.

3. Log in to the SV4PC cluster by using the superuser account (see Figure 3).

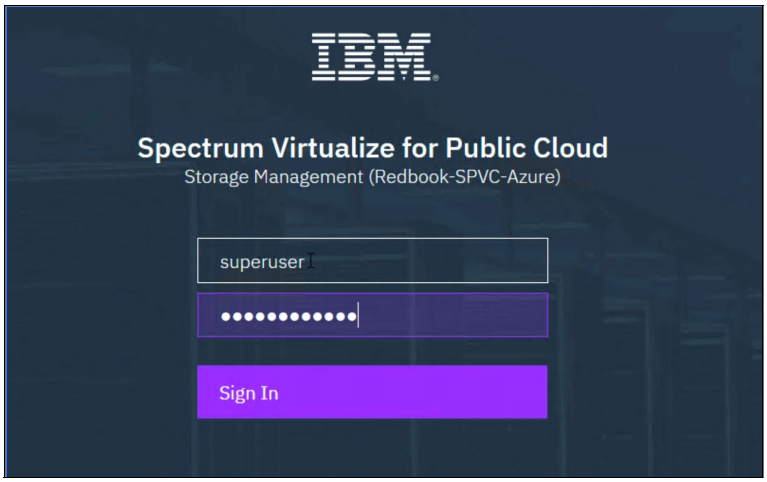


Figure 3 IBM Spectrum virtualized for public cloud, login

This host (`VM-Hemanand`) also was installed by using IBM Copy Services Manager software (the log in window is shown in Figure 4).

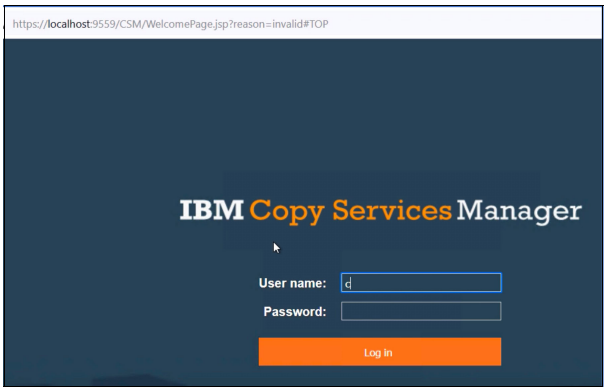


Figure 4 IBM copy service manager login window

For more information about installing IBM Copy Services Manager, see refer this IBM Documentation web page.

After IBM Copy Services Manager is installed, complete the following steps to build a Cyber security solution using IBM SV4PC on Azure and IBM Spectrum Virtualize Safeguarded Copy feature:

1. Create a Safeguarded Pool on IBM Spectrum Virtualize for Public Cloud in Azure.
2. Set up the volume group and Safeguarded policies.
3. Install and configure IBM Copy Services Manager.
4. Safeguard back up the production volume.
5. Restore/Recover data from immutable safeguarded copy snapshots.
6. Restore from Safeguarded Backup.
7. Replicate the IBM Spectrum Virtualize for Public Cloud storage volume with IP replication between sites in Azure.

Creating a Safeguarded Pool on IBM Spectrum Virtualize for Public Cloud in Azure

To configure the Safeguarded Copy function, the first step is to create to the Safeguarded backup location. The Safeguarded backup location is created as a special child pool.

A Safeguarded backup location is a child pool in each parent pool where the source volume is located. The Safeguarded backup location stores Safeguarded backup copies.

The Safeguarded Copy function supports the ability to create cyber-resilient point-in-time copies of volumes that cannot be changed or deleted through user errors, malicious actions, or ransomware attacks. The Safeguarded backup location can contain multiple versions of volume data that is backed up based on different copy intervals and retention to cover various recovery point objectives.

To create a Safeguarded backup location, complete the following steps:

Note: In this lab setup, we deployed the following SV4PCs in Azure Site A and Site B (see Figure 1 on page 5):

- Site A: `Sol-SVPC`
- Site B: `Rebook-SVPC-Azure`

1. Log in to the `Redbook-SVPC-Azure` cluster management GUI.
2. In the management GUI, select **Pools** → **Pools**.
3. Right-click a parent pool and select **Create Child Pool**.
4. On the Create Child Pool page, enter a name of the child pool.

   If the parent pool is a standard pool, enter the amount of capacity that is dedicated to the child pool. If the parent pool is a data reduction pool, the child pool shares capacity with the parent pool, as shown in Figure 5 on page 10.

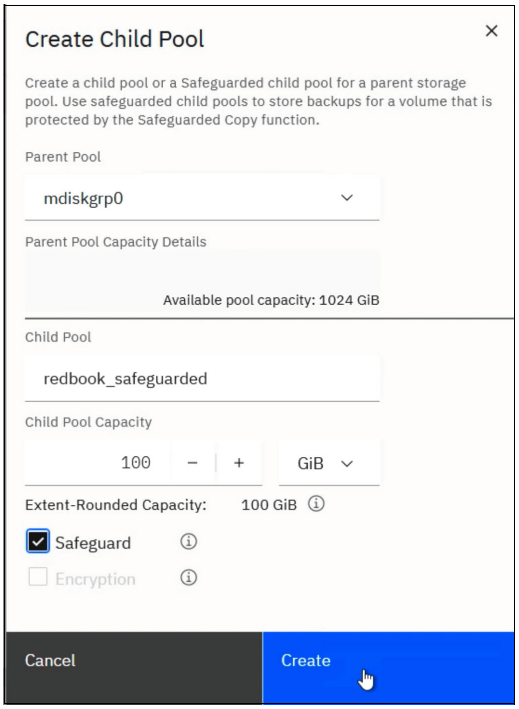


Figure 5 Creating a child pool

5. Select **Safeguard** to indicate that the child pool is used as the Safeguarded backup location for immutable backup copies of source volumes
6. Click **Create**. Child pools that are used as Safeguarded backup locations are marked with a shield icon in the Pools page, as shown in Figure 6.

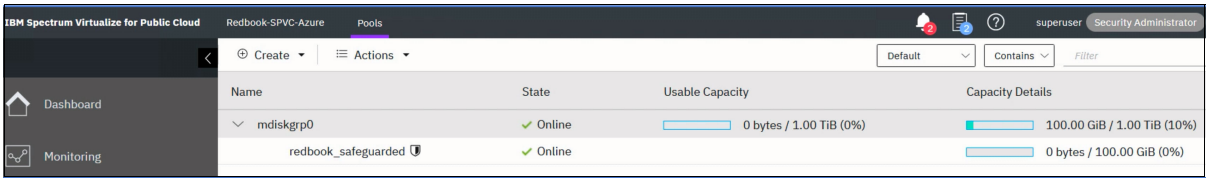


Figure 6 Child pool created in the parent pool

In this lab setup, the `redbook_safeguarded` child pool is configured in the parent `mdiskgrp0`.

Setting up a volume group and Safeguarded policies

Volume groups are used to manage groups of related volumes to which a Safeguarded Copy Policy is attached.

Volume groups create a set of source volumes that can span different pools and are copied collectively to Safeguarded backup child pools with Safeguarded Copy function. Before you create a volume group, determine which source volumes you want to protect.

To create a volume group, complete the following steps:

1. In the management GUI, select **Volumes** → **Volumes Groups**.
2. Click **Create Volume Group**.

   On the Create Volume Group page, enter a name of the volume group. From the list of volumes, select of the volumes that you want in the volume group.

   Note: If you select volumes in a parent pool that do not contain a child pool to use as the Safeguarded backup location, select **Navigate to Pools**. For each parent pool with source volumes, you must configure a child pool as the Safeguarded backup location.

3. Click **Create Volume Group**. In this lab setup, the volume group is created with the name `redbook_safeguarded_policy`, as shown in Figure 7.

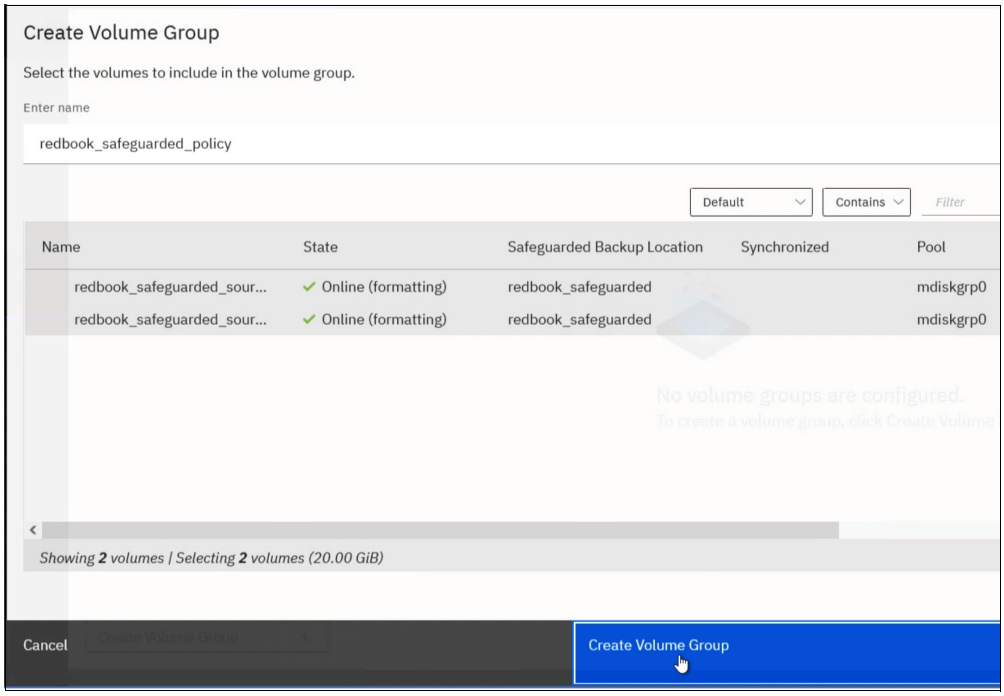


Figure 7 Creating a volume group and adding volumes

4. After the volume group is created, add source volumes to the volume group. In this example, the following source volumes were added to the volume group:
   - Volume 1: `redbook_safeguarded_source0`
   - Volume 2: `redbook_safeguarded_source1`

Figure 8 shows the two production volumes that were added to the `redbook_safeguarded_policy` volume group.

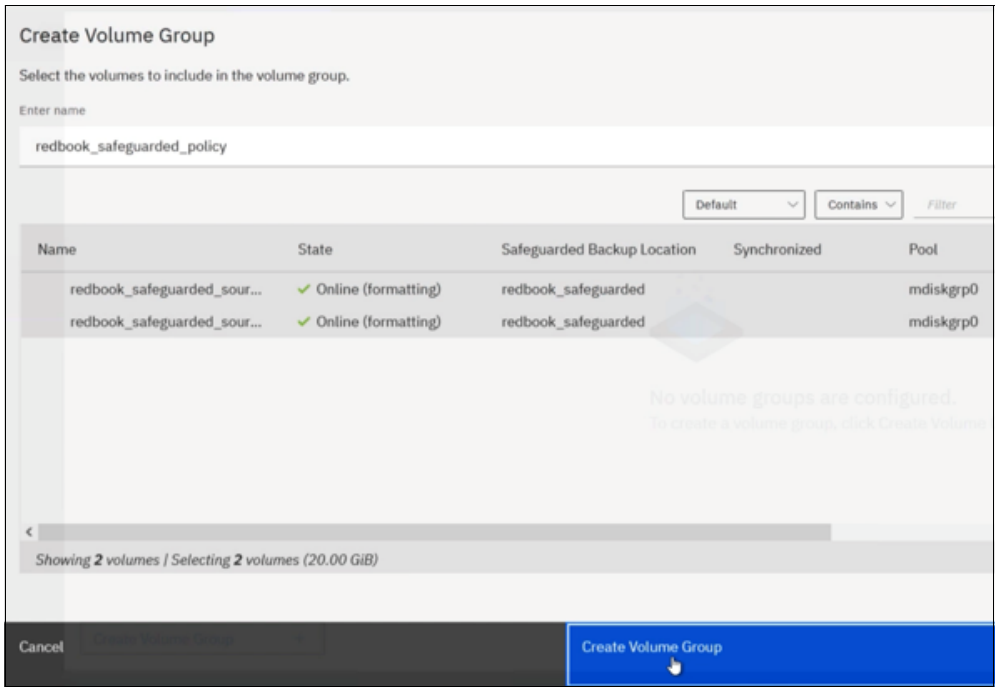


Figure 8 Volumes added to volume group

Assigning a Safeguarded Policy

A Safeguarded policy controls the creation, retention, and expiration of Safeguarded backup copies of source volumes.

The management GUI supports displaying predefined and user-defined Safeguarded policies. Although the management GUI does *not* support creating user-defined Safeguarded policies, you can use the **`mksafeguardedpolicy`** command to create user-defined policies.

The predefined policies that are in the system are shown in Figure 9.

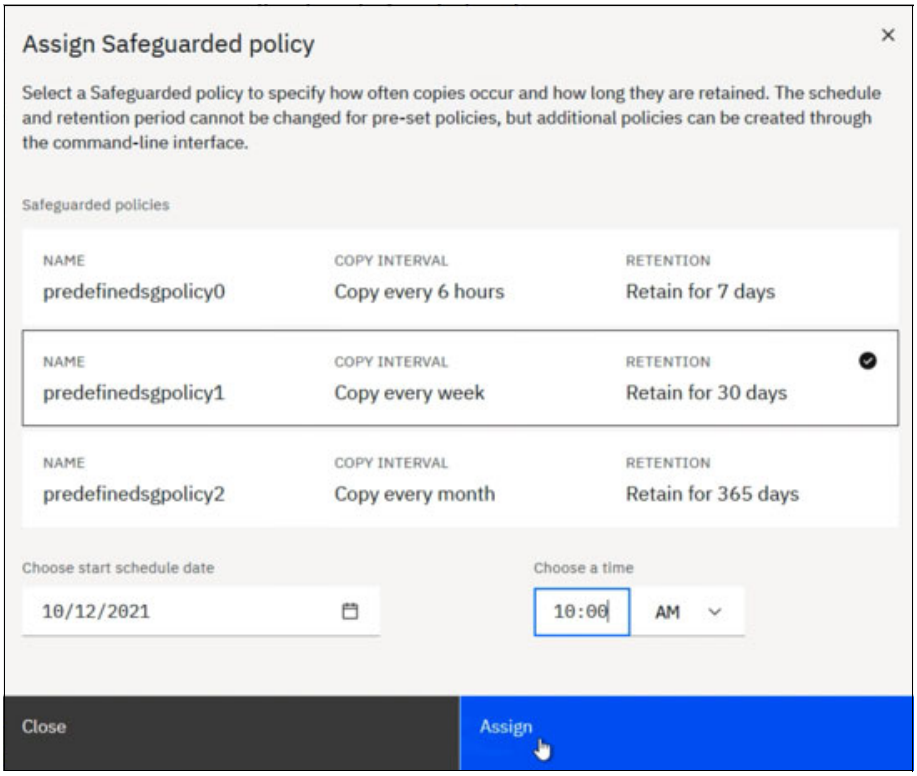


Figure 9 Predefined safeguarded policies

To assign a Safeguarded backup policy to a volume group, complete the following steps:

1. In the management GUI, select **Volumes** → **Volumes Groups**.
2. Select the volume group that you want to assign a predefined policy to and then, select **Group Actions** → **Assign Safeguarded policy**.
3. Select one of the predefined Safeguarded policies (in this example. `Predefinedsgpolicy1` is selected (see Figure 9).

   For this policy, Safeguarded backup copies are created weekly and retained for a month.

Note: These predefined policies cannot be changed or deleted. If you create user-defined Safeguarded backup policies by using the **mksafeguardedpolicy** command, IDs start after the predefined policies.

The system supports a maximum of 30 Safeguarded backup policies with three predefined policies and 27 user-defined policies. If you create user-defined Safeguarded backup policies in the CLI, you can view and select these policies within the management GUI. Neither interface supports changes to predefined Safeguarded backup policies.

4. Select a date and time for when you want to start creating Safeguarded backups that use the policy.
5. Click **Assign**.

   After the Safeguarded policy is assigned to the volume group, the status of the volume group displays as `Safeguarded-scheduled`, as shown in Figure 10.

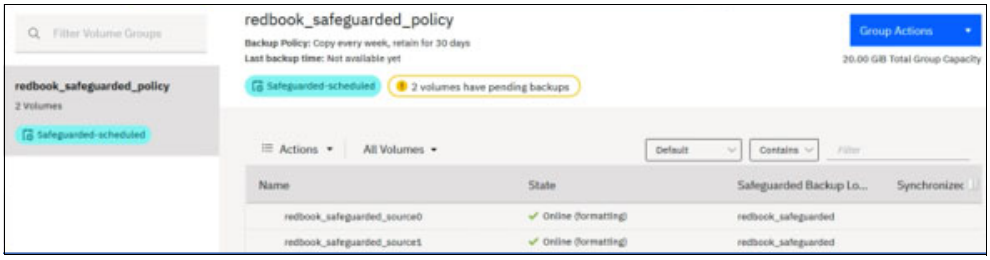


Figure 10 Safeguarded policy scheduled

This status indicates that the policy is assigned, but the Safeguarded backup has not started. When Safeguarded backups are stored on the Safeguarded backup location, the status of volume group displays Safeguarded. After Safeguarded copies are added to the Safeguarded location, users with Administrator role or lower cannot delete any parent pool with a Safeguarded location.

Installing and configuring IBM Copy Services Manager

This section describes installing and configuring IBM Copy Services Manager.

IBM Copy Services Manager automates the creation of Safeguarded backup copies according to a schedule that is defined in a Safeguarded policy and the recovery and restoration operations with Safeguarded backup copies.

Ensure that the following requirements are met for IBM Copy Services Manager:

- IBM Copy Manager for IBM Spectrum Virtualize is purchased, which includes IBM Copy Services Manager version 6.3.0 or later. This license option is available through iERP/AAS, IBM Passport Advantage®, or your IBM Sales team.
- IBM Copy Services Manager version 6.3.0 or later is available for download from this IBM Support web page.

  After you download IBM Copy Services Manager, complete the instructions for your installation. IBM Copy Services Manager supports several installation options on different environments. For more information, see this IBM Documentation web page.

Creating an Administrator user for IBM Copy Services Manager

Before you can establish the IBM FlashSystem as a connection endpoint in IBM Copy Services Manager, a user with an Administrator role must be configured on the IBM FlashSystem.

For auditing, it is recommended that you create an Administrator user to configure the Safeguarded Copy function. Users with this role are limited in how they can manage and interact with Safeguarded Copy operations. The IBM Copy Services Manager uses this role to create FlashCopy® mappings between the source volumes and the Safeguarded backup copies on the IBM® FlashSystem.

To create an administrator user on IBM SV4PC for IBM Copy Services Manager, complete the following steps:

1. Log in to the `Redbook-SVPC-Azure` cluster management GUI.
2. In the management GUI, select **Access** → **Users by Groups** → **Create User**.
3. On the Create Users page, enter the name of the user, select the Administrator group and then, select **Local**.
4. To connect to the management GUI by using this user, enter and confirm a password. Click **Create**.

In this example, the `csm_user` user is created, which is used for IBM Copy Services Manager, as shown in Figure 11.

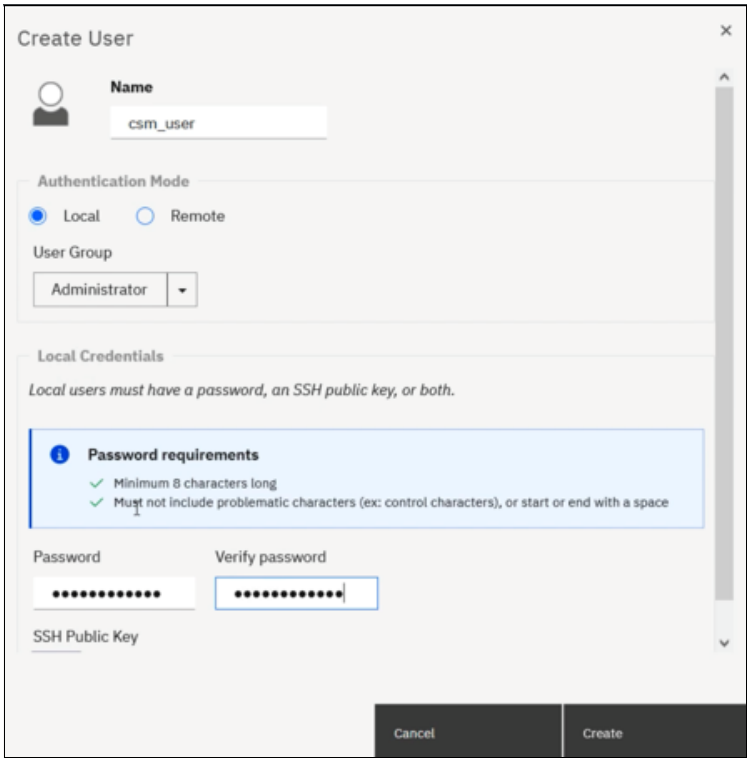


Figure 11 Creating an admin user for IBM Copy Services Manager

Creating a connection to the system in IBM Copy Services Manager

To use the Safeguarded Copy function, you must create a connection to the system in the IBM Copy Services Manager interface. Complete the following steps:

1. Log in to IBM Copy Services Manager at `https://{CSM_SERVER_IP/HOST}:9559/CSM`, where *CSM_SERVER_IP* is the IP address or Host name of IBM Copy Services Manager instance.
2. Select **Storage** → **Storage Systems**.
3. On the Storage Systems page, select **Add Storage Connection**.
4. Click one of the following options based on your product:
   - FlashSystem Spectrum Virtualize
   - SAN Volume Controller
   - IBM Storwize® Family
5. On the Connections page, enter the following information for your system:
   - Cluster IP or Domain Name
   - Management IP address or domain name for your system
   - Username for the Administrator user for the system
   - Password that is associated with the Administrator user for the system

   Click **Finish**.
6. On the Storage Systems page, verify that Local Status for the connection is `Connected`, as shown in Figure 12.

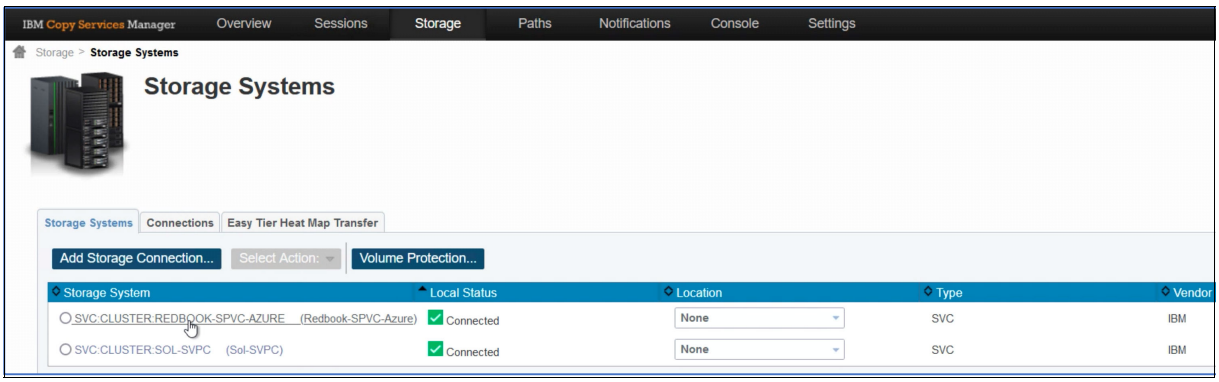


Figure 12 Creating a connection to IBM FlashSystem in IBM Copy Service Manager

After a connection is established, IBM Copy Services Manager automatically detects volume groups with Safeguarded policies and schedules the backup copies.

IBM Copy Services Manager queries the system every 5 minutes to process Safeguarded policies. The start time that is defined in the Safeguarded backup policy must factor in the possible 5-minute delay.

When IBM Copy Services Manager detects new a Safeguarded backup policy for a volume group, it creates the session and scheduled task to create and manage the Safeguarded backup copies.

To view Safeguarded backup copies in IBM Copy Services Manager interface, select **Sessions**.

The session name is based on the name of the volume group and the storage system, In this example (see Figure 13), the `redbook_safeguarded_policy` volume group that is created on IBM SV4PC is automatically visible as a session in IBM Copy Services Manager, as shown in Figure 13.

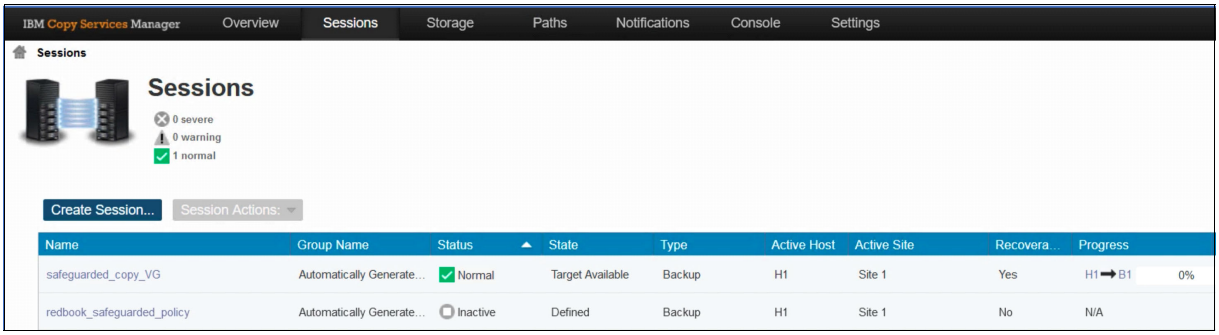


Figure 13 Safeguarded copy session automatically visible in IBM copy service manager

As part of this session, it includes two volumes, which are part of volume group (see Figure 14).

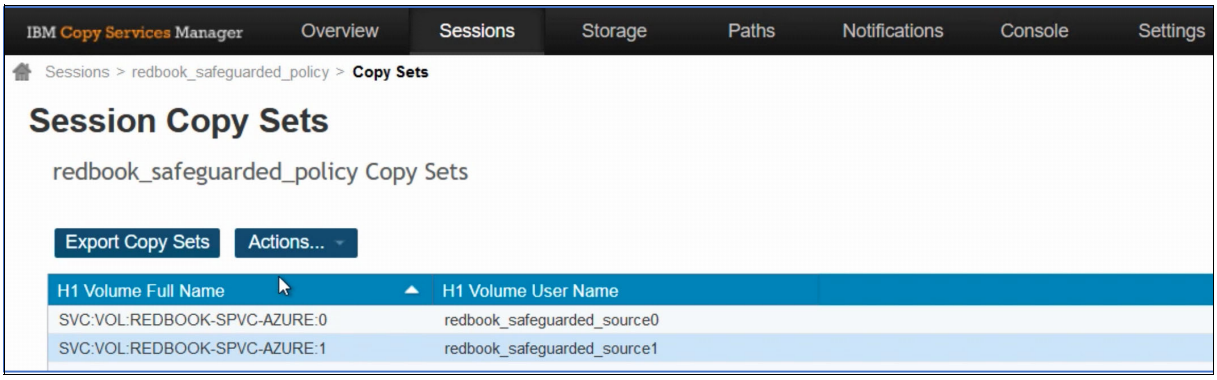


Figure 14 Volume information for the session

The IBM Copy Services Manager session details (see Figure 15) includes information about the Safeguarded policy that is set on the volumes for the backup and retention.

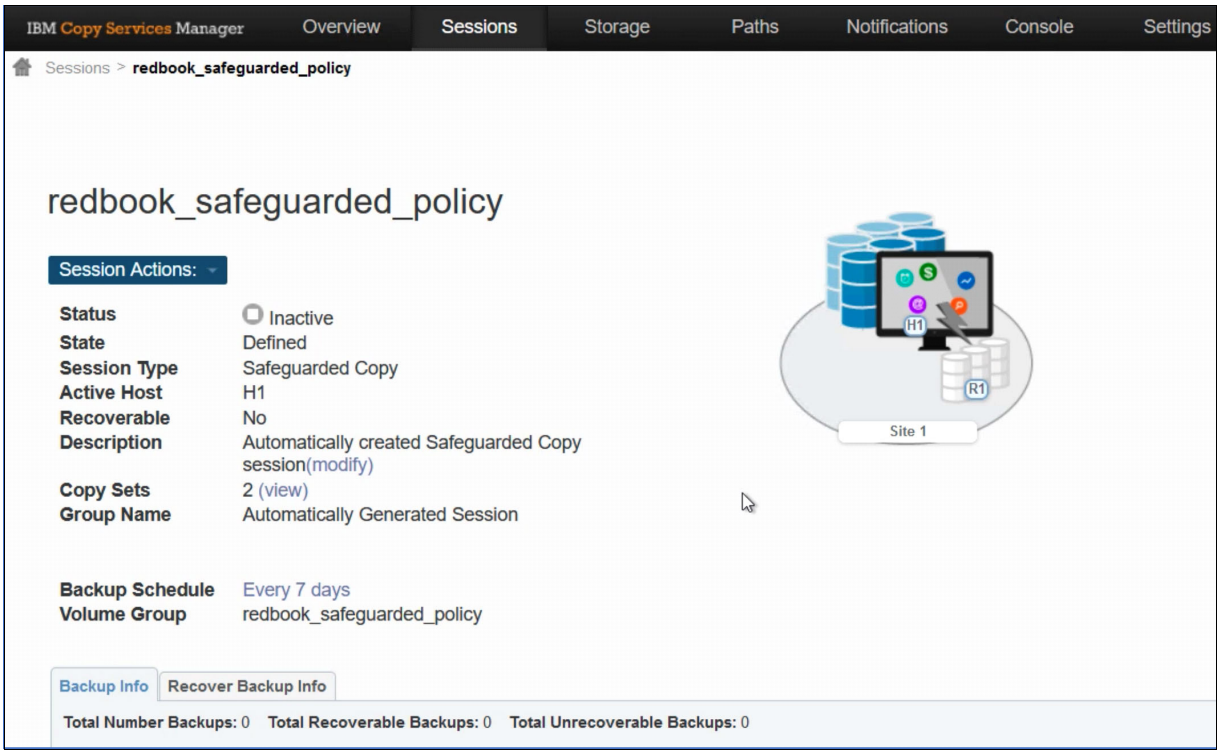


Figure 15 Policy information for the safeguarded volume group

Safeguarded backup of production volumes in IBM Spectrum Virtualize for Public Cloud on Azure

In this environment, the Safeguarded backup of the following production volumes is created: one volume is named `redbook_Safeguarded_source0`; second volume is named `redbook_safeguarded_source1`.

The Safeguarded backup is a crash IBM consistent FlashCopy. To create application consistency, the database must be quiesced or database is made read-only before the backup is taken.

In this example, we show the ad hoc backup that was created to demonstrate the Safeguarded backup; otherwise, the backup runs according to the schedule that is selected.

Complete the following steps:

1. Log in to IBM Copy Services Manager at `https://{CSM_SERVER_IP/HOST}:/:9559/CSM`, where is the IP address or domain name of IBM Copy Services Manager instance in your network.
2. Select **Sessions** → **redbook_safeguarded_policy**. Click **Session Actions** → **Commands** → **Backup** (see Figure 16).

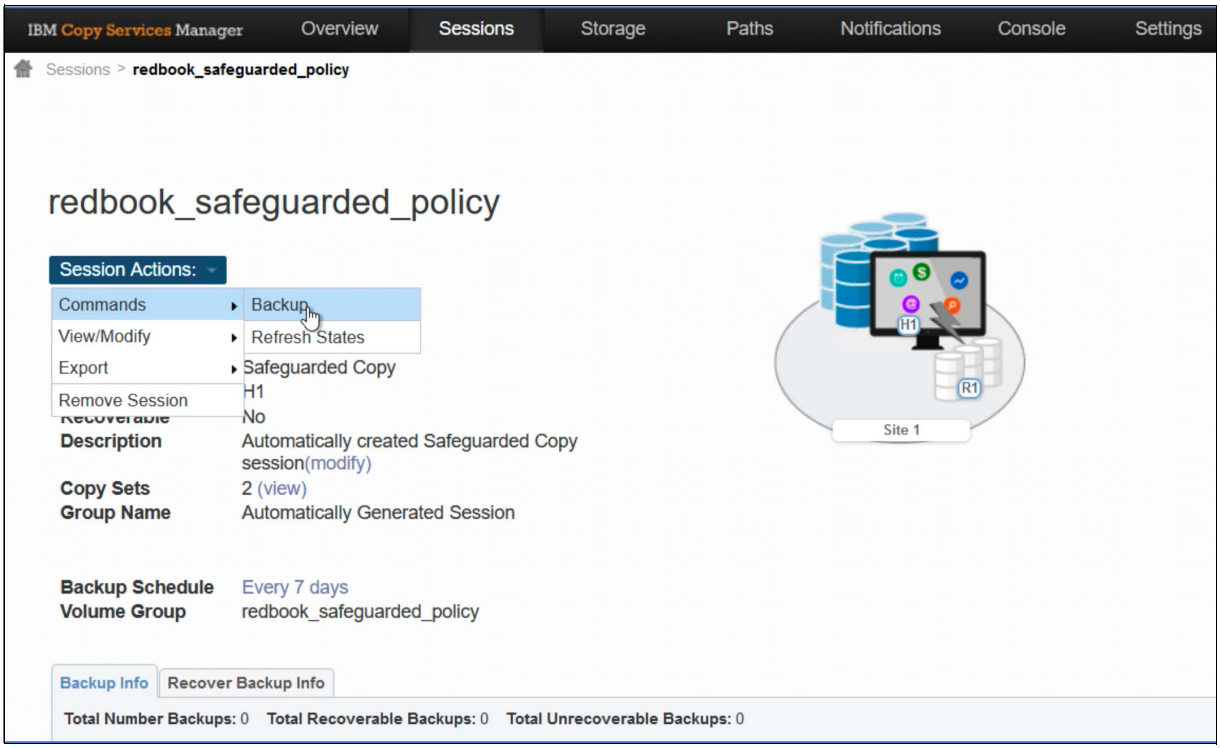


Figure 16 Ad hoc backup for the volume group

The Safeguarded backup copy is created by using IBM Copy Services Manager according to the schedule and Safeguarded policy that is assigned to volume group, as shown in Figure 17.

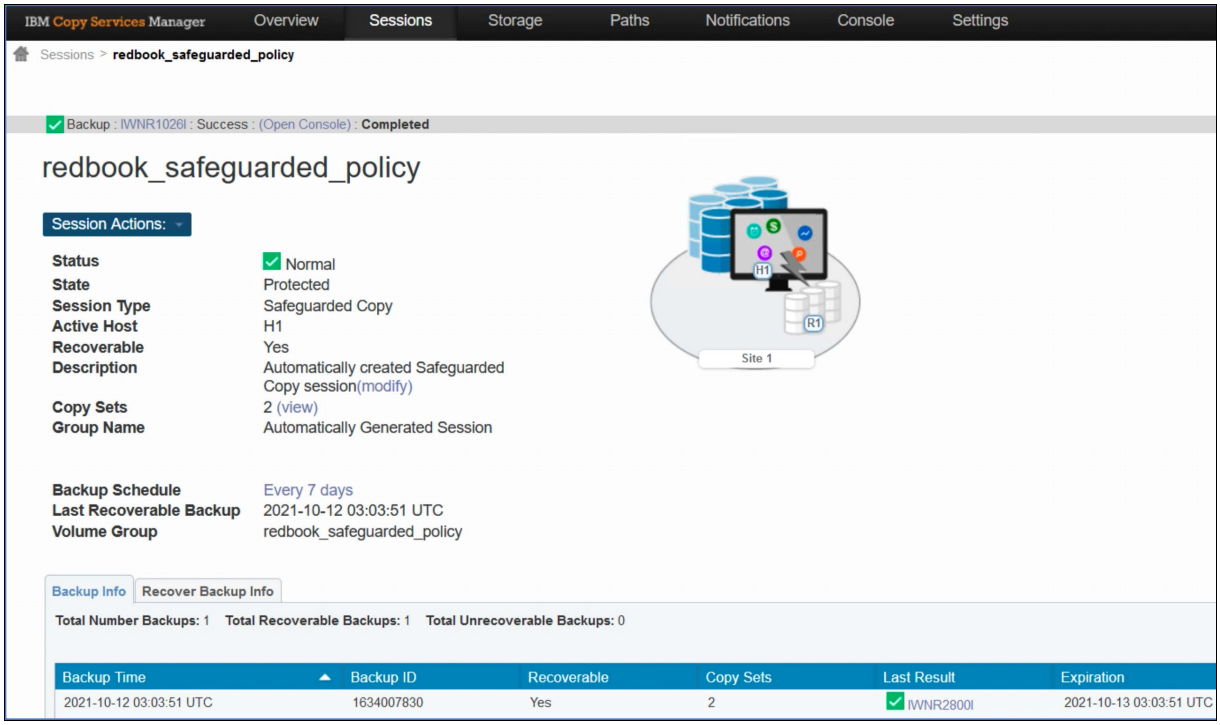


Figure 17 Safeguarded backup completed per the backup policy assigned

3. Log in to the `Redbook-SVPC-Azure` cluster management GUI and check the status of backup volumes. Click **Pools**.

   The backup volumes are created in the Safeguarded backup location (also referred to as *child pool*), as shown in Figure 18.

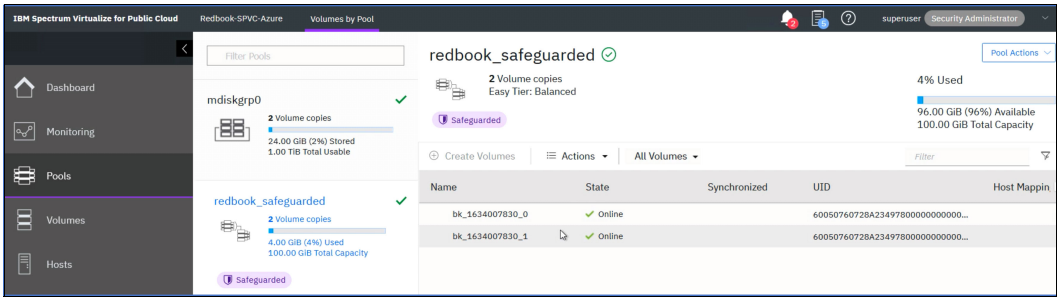


Figure 18 Immutable backup copies created

These immutable volumes in the Safeguarded location cannot be deleted, modified, or assigned to the host for read/write.

4. Check the status of source volume as Safeguarded, as shown in Figure 19.

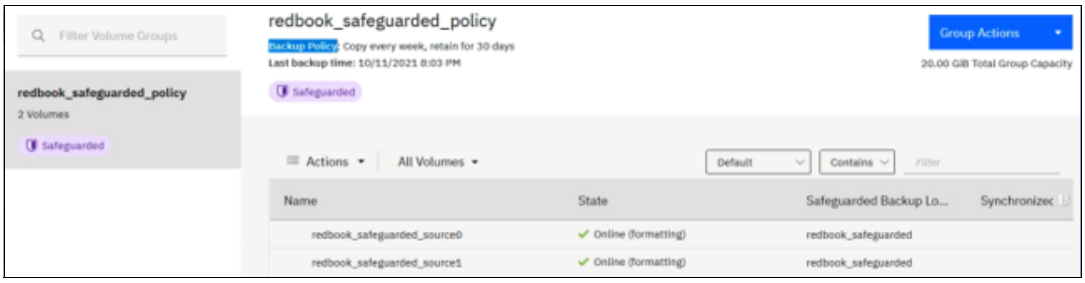


Figure 19 Status of the volumes in volume group as Safeguarded

Restoring and recovering data from immutable safeguarded backups

IBM Copy Services Manager provides an automated process that is used for testing that is called the Recover Backup action. The Recover Backup action creates recovered versions of Safeguarded backup copies that you can map to a host and verify that host applications run correctly.

To test Safeguarded backup copies, complete the following steps:

1. Log in to `https://{CSM_SERVER_IP/HOST}:9559/CSM`, where `https://{`*`CSM_SERVER_IP`*`/HOST}:9559/CSM`, where *`CSM_SERVER_IP`* is the IP address or Host name of IBM Copy Services Manager instance.
2. On the Sessions Overview page, select **Sessions**.
3. On the Sessions page, select the volume group that contains Safeguarded backup copies that you want to recover.

4. Select which generation of the backup you want to recover; in this example we are restoring the latest backup, as shown in Figure 20 and Figure 21.

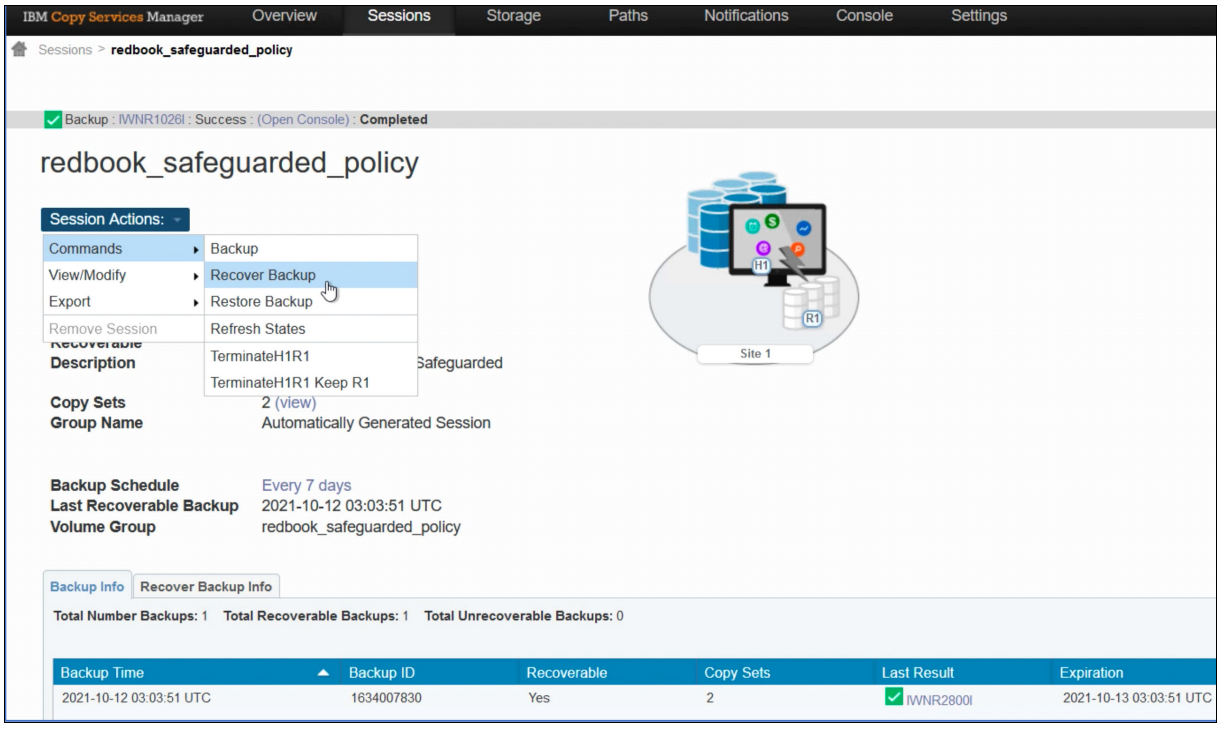


Figure 20 Recover backup from the latest backup

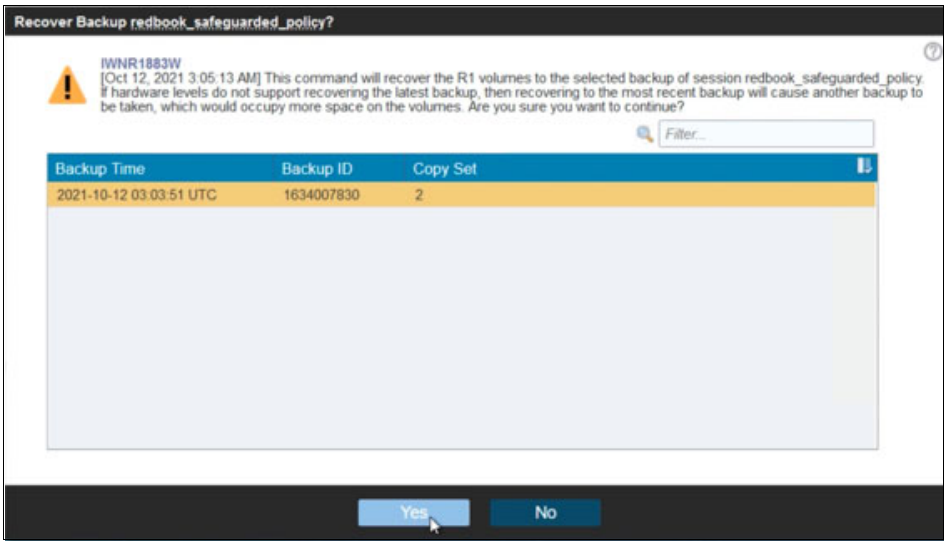


Figure 21 Recovering the latest copy backup

After the recovery completes, the recovery happens on the new volume in the parent pool where the source volume are originally present (see Figure 22).

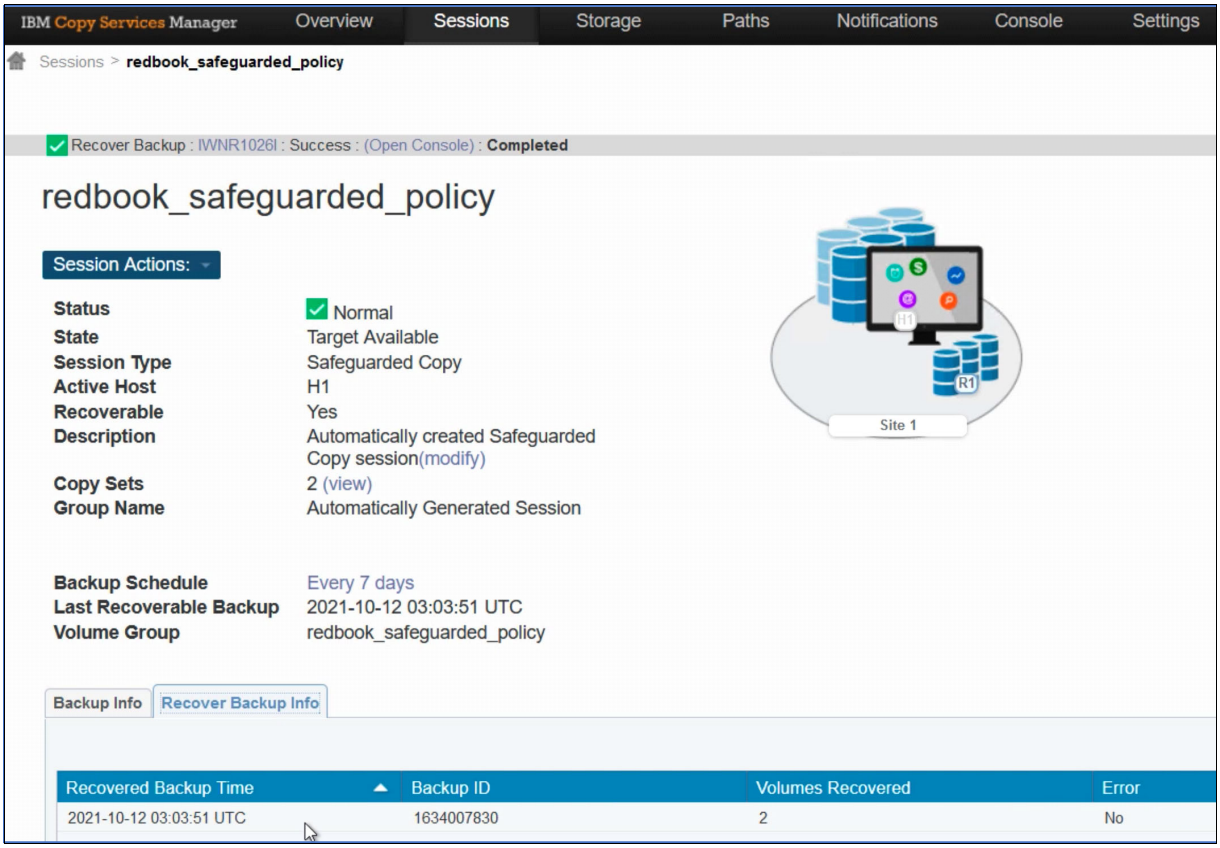


Figure 22 Status of the recovered volume

5. Log in to the IBM SV4PC storage (`https://40.10.1.28:8443/login`), and check the status of recovered volumes, as shown in Figure 23.

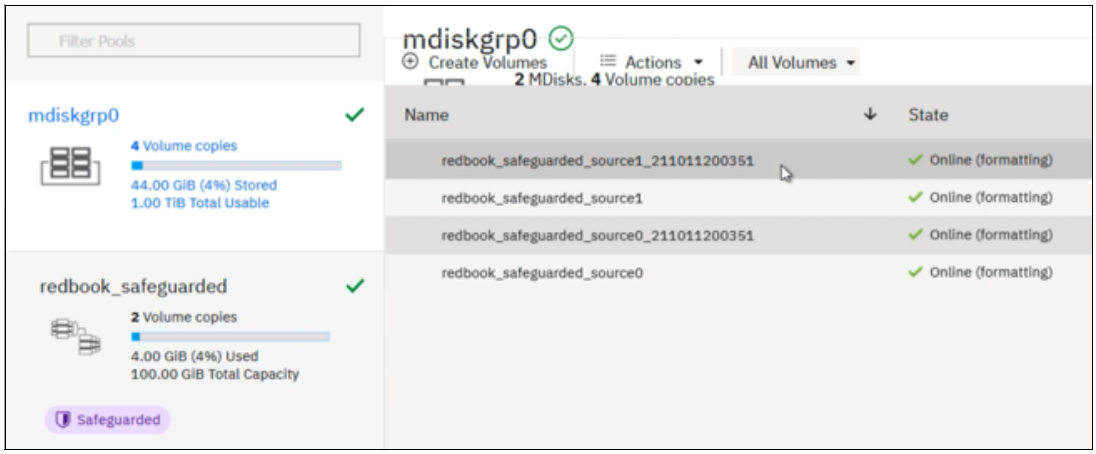


Figure 23 Recovered volume information

For more information about how to log in to IBM SV4PC Cluster, see “Single-site scenario: Deploy IBM Spectrum Virtualize for Public Cloud in Azure” on page 7.

The newly recovered volumes that are shown in Figure 23 on page 23 can be mapped to the host to check for data integrity and consistency:

- `redbook_safeguarded_source0_211011200351`
- `redbook_safeguarded_source1_211011200351`)

Restoring from a Safeguarded backup copy

If your production data was compromised by a cyberattack, you can restore data to the source volumes by using a Safeguarded backup. The IBM Copy Services Manager automates and simplifies the process of testing and restoring compromised data from a Safeguarded backup copy.

Before you can restore data to the source volume with a Safeguarded backup copy, ensure that you fully test the Safeguarded backup copies that are associated with the compromised source volume by recovering to an alternative volume and validating the data on that recovery volume.

Multiple versions of Safeguarded backup copies can exist, and some versions can include malware or damaged data. The restore operation copies all source volume data with the version of the Safeguarded backup copy from which you are restoring.

To restore Safeguarded backup copies, complete the following steps:

1. Log in to `https://{CSM_SERVER_IP/HOST}:9559/CSM`, `https://{`*`CSM_SERVER_IP`*`/HOST}:9559/CSM`, where *`CSM_SERVER_IP`* is the IP address or Host name of IBM Copy Services Manager instance
2. On the Sessions Overview page, select **Sessions**.
3. On the Sessions page, select the volume group that contains the Safeguarded backup copies that you want to restore.
4. Select **Session Actions** → **Command** → **Restore Backup**.
5. On the Restore Backup page, select the version of the Safeguarded backup copy that you want to restore. Safeguarded backup copies are displayed by their backup time from the most recent to the latest version. Restored Safeguarded backup copies replace the source volumes that is defined in volume group.
6. Click **Yes**.

Two-site Airgap scenario: Replicating the IBM Spectrum Virtualize for Public Cloud storage volume between two sites in Azure

In this section of two-site air-gap scenario, we describe the configuration steps that were done in the lab setup. This setup was deployed IBM SV4PC on Site A and Site B in Azure, as described in the architecture (see Figure 1 on page 5).

In this demonstration, we added two volumes on IBM SV4PC in Site A and created similar size volumes on IBM SV4PC in Site B. We also replicated the volumes by using native storage-based replication (global mirror) from IBM SV4PC storage

After the volumes are replicated, we create a Safeguarded Copy of the volume at Site B and create a Safeguarded backup. After the Safeguarded backup is completed, we started a recovery of latest Safeguarded backup copy and assigned a recovered volume to the restore VM. Then, we checked the sample data that is available on the recovered volumes:

- `Sol-SVPC`: Name of the SV4PC storage in Site A in Azure region
- `Redbook-SVPC-Azure`: Name of the SV4PC storage in Site B Azure region

Complete the following steps:

Note: Before creating the partnership, ensure that you set up the IP address and portset for remote copy. For more information, see this IBM Documentation web page.

1. Set up an IP replication between two sites: `Sol-SVPC` (Site A) and `Redbook-SVPC-Azure` (Site B).
2. Log in to the `Sol-SVPC storage` (Site A), select **Copy-Services** and then, click **Remote Copy**. Click **Create Partnership** → **Two site partnership** → **IP**. Enter the information as shown in Figure 24 on page 26. Click **Create** to set up the partnership.

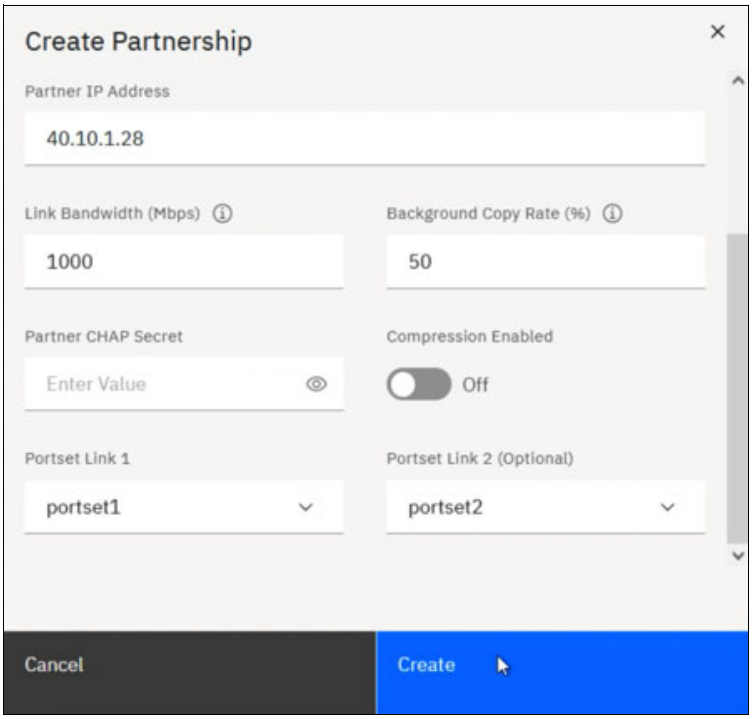


Figure 24 Creating partnership Sol-SVPC (Site A)

A message is displayed when the creation process completes (see Figure 25).

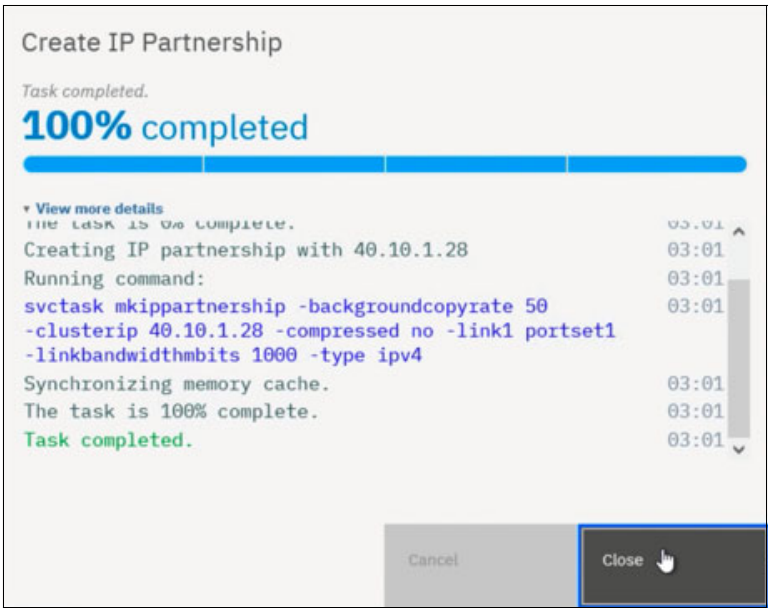


Figure 25 Partnership creation process complete (Site A)

3. Log in to the `Redbook-SVPC-azure` storage (Site B). Select **Copy-Services** and then, click **Remote Copy**. Click **Create Partnership** → **Two site partnership** → IP. Enter the information as shown in Figure 26. Then, click **Create** to set up the partnership.

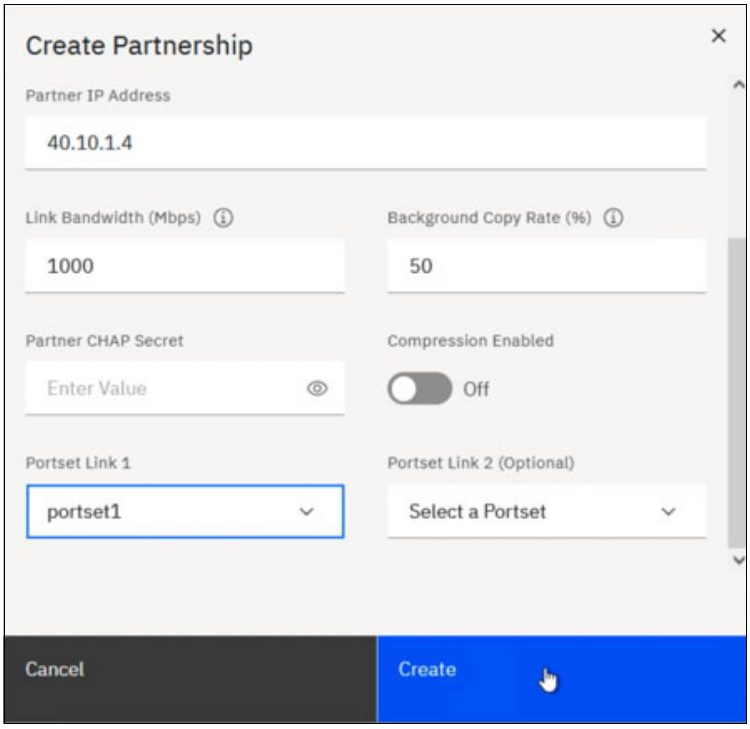


Figure 26 Creating partnership Redbook-SVPC-Azure (Site B)

A message is displayed when the creation process completes (see Figure 27).

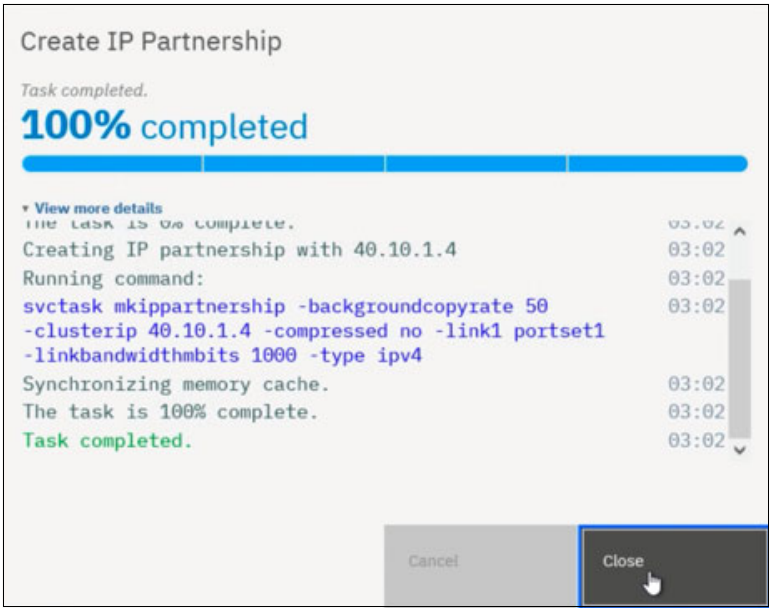


Figure 27 Partnership creation process complete (Site B)

4. Ensure that you added iSCSI hosts and volumes to the hosts. In our lab setup, two hosts are available (`VM-Hemanand` and `Restore-VM-Hemanand`).

We added two Volumes to these hosts and replicated the volumes by using native replication from IBM SV4PC storage. After the volumes are replicated, we create a Safeguarded Copy of the volume at Site B and a Safeguarded backup.

After the Safeguarded backup is completed, we start a recovery of latest Safeguarded backup copy and assign a (recovered volumes) to the restore VM. Then, we check the sample data that is available on recovered volumes.

As described in Step 4, to add iSCSI host and volumes to the storage, Figure 28 shows the sample iSCSI connection from the `Restore-VM-Hemanand` where targets are added in the iSCSI configuration of the Windows hosts. In a similar way, you must add targets and a configuration to the Windows host (see Figure 28).

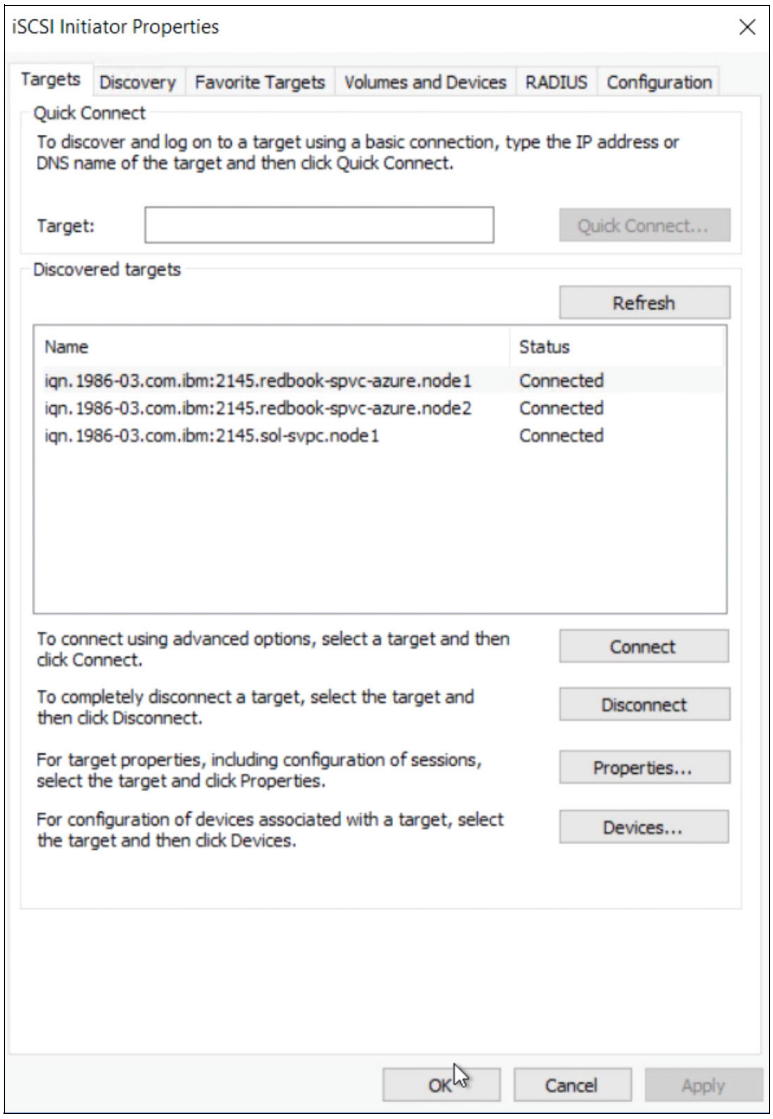


Figure 28 Sample iSCSI configuration from Windows host

5. After you set up the remote replication and added iSCSI hosts, start the replication of the volumes. Log in to the source side SV4PC; that is. Site A (Sol-SVPC). Select **Copy Services** → **Remote Copy** → **Add Consistency group**. Select the location of the target volumes and then, click **Add** (see Figure 29).

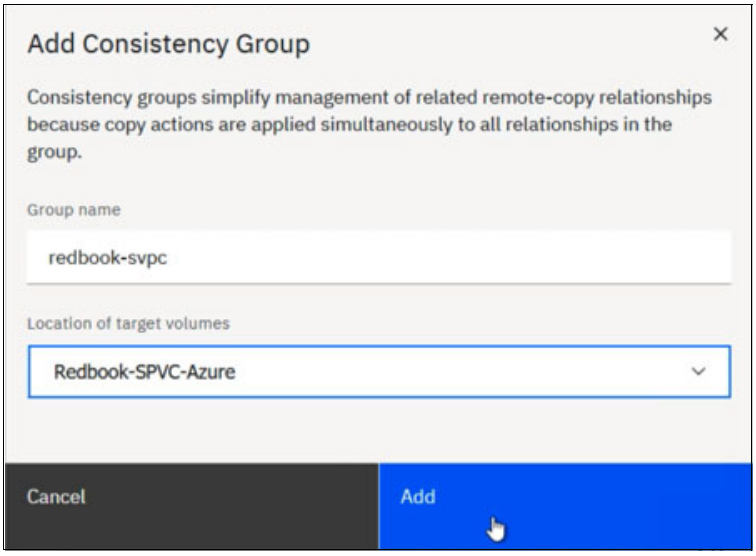


Figure 29 Add Consistency Group window

Figure 30 shows the status of the configured consistency group.

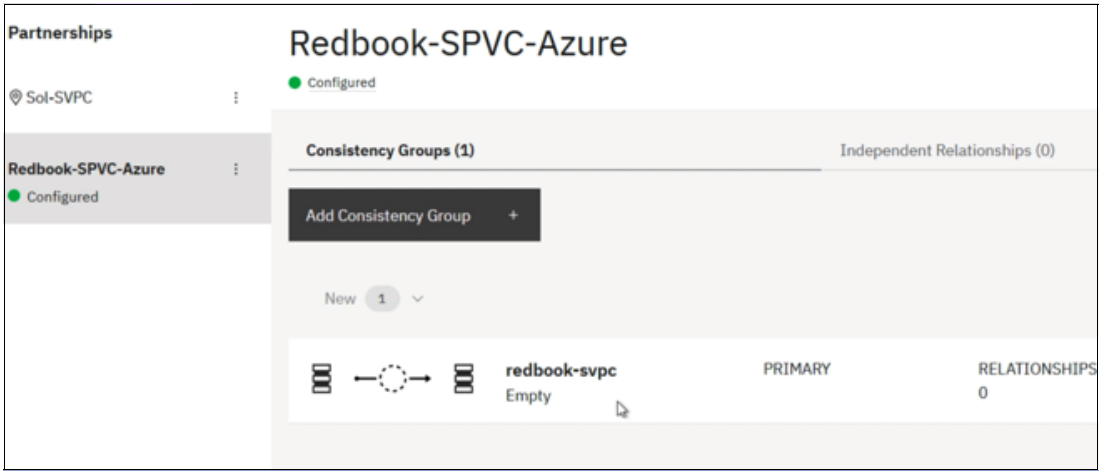


Figure 30 Consistency group configured

6. To create a relationship, log in to the Sol-SVPC and select **Copy Services**. Select the `Redbook-SVPC-Azure` storage in the Remote copy tab. Click **Create Relationship** and then, Select **Global Mirror** and then, the **use consistency protection** option. Click **Next**.
7. Click another system and select `Redbook-SVPC-Azure`. Then, click **Next** → **Master**. In the drop-down menu, select **Sol-SVPC-Source1** and **Auxiliary**. In the drop-down menu, select **Sol-SVPC-Target1**. Click **Add** and then, select **No, do not add master change volume**. Click **Finish**.
8. In a similar way add, volumes to the relationship `Sol-SVPC-Source0` to `Sol-SVPC-Target0`. Click **Next** and then, select **No, the volumes are not synchronized**. Click **Next**.
9. Select **Yes, Start copying**. Click **Finish**. After the relationship is created, click **Close**.

Before the relationship is created, ensure that the correct volumes were created on SVPC on both sites. In our lab, we set up the following volumes that were used for source and target volumes (see Figure 31 and Figure 32):

- Sol-SVPC: Sol-SVPC-Source0
- Sol-SVPC: Sol-SVPC-Source1
- Rebook-SVPC-Azure: Sol-SVPC-target0
- Rebook-SVPC-Azure: Sol-SVPC-target1

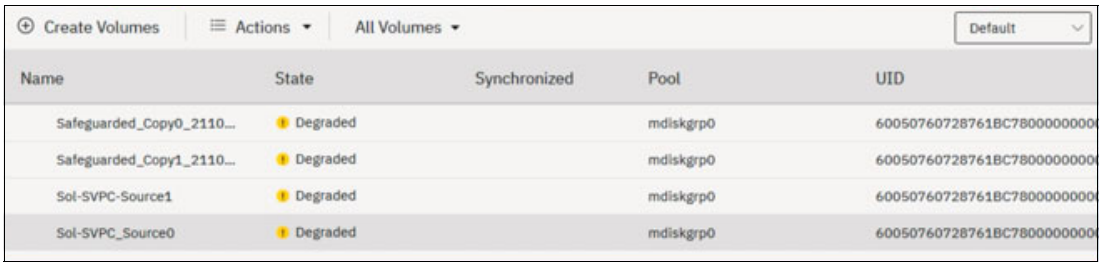


Figure 31 Source volume information

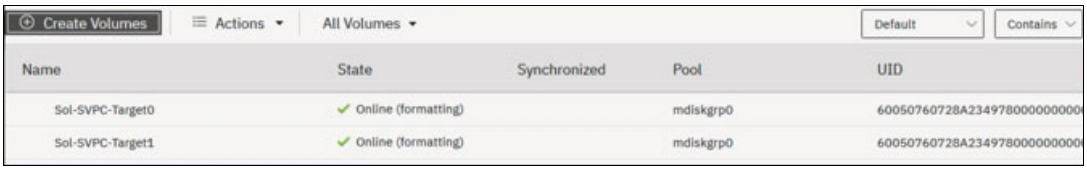


Figure 32 Volume target information

Figure 33 shows the status of relationship and the state as `Inconsistent Copying`.

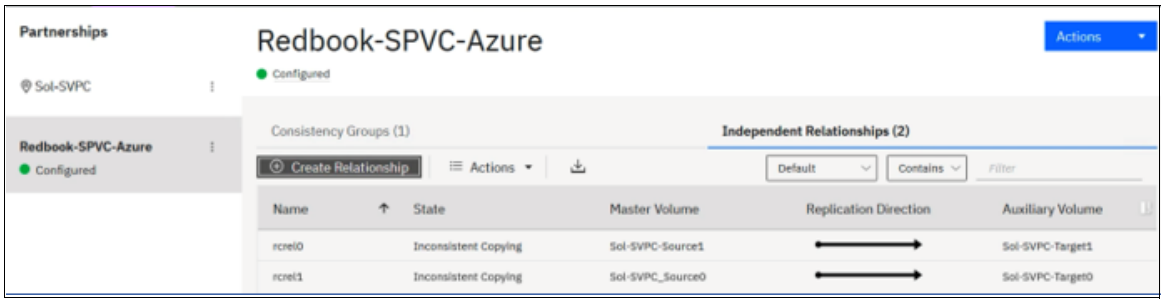


Figure 33 Relationship created for two volumes

10. To add the volume relationship to a consistency group, select **Copy Services** → **Remote Copy**. Select **Redbook-SVCP-Azure** and then, click **Independent Relationship**.

11. Select the Master volume and then, right-click and select **Add to Consistency Group** (see Figure 34).

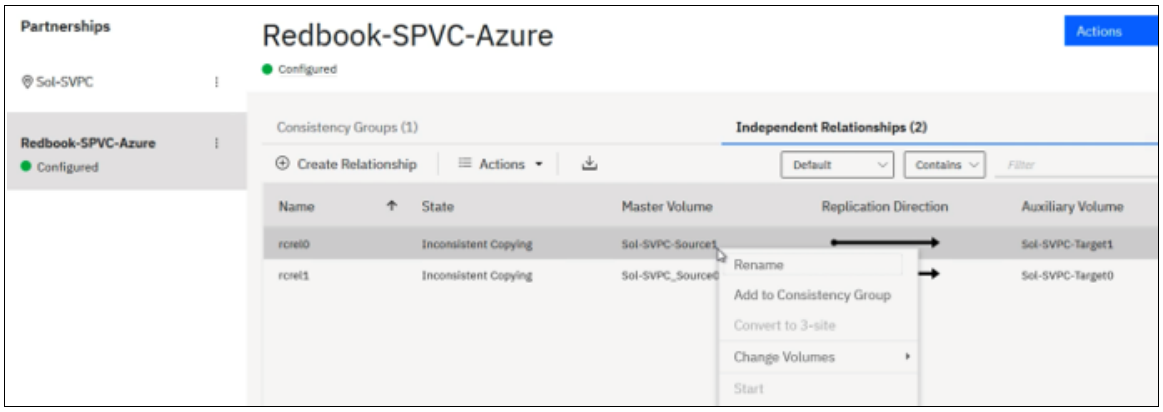


Figure 34 Adding relationship volumes to consistency group

12. Check the state of the replication.

    The `Inconsistent Copying` status changes (see Figure 35) to `Consistent Synchronized` after initial synchronization is achieved (see Figure 36 on page 32).

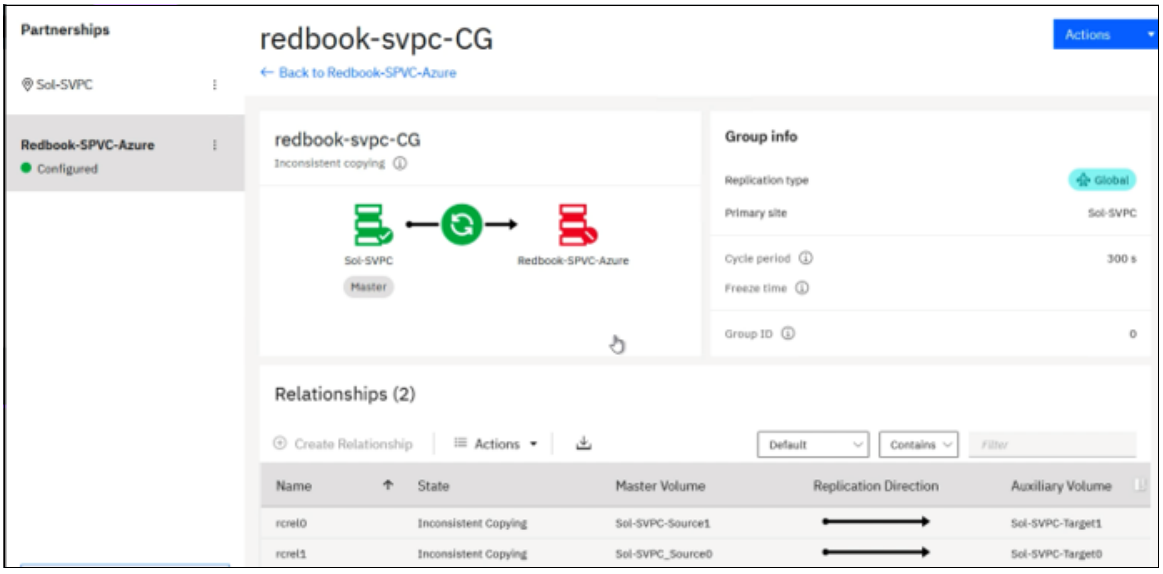


Figure 35 Copy status displayed as consistent copying

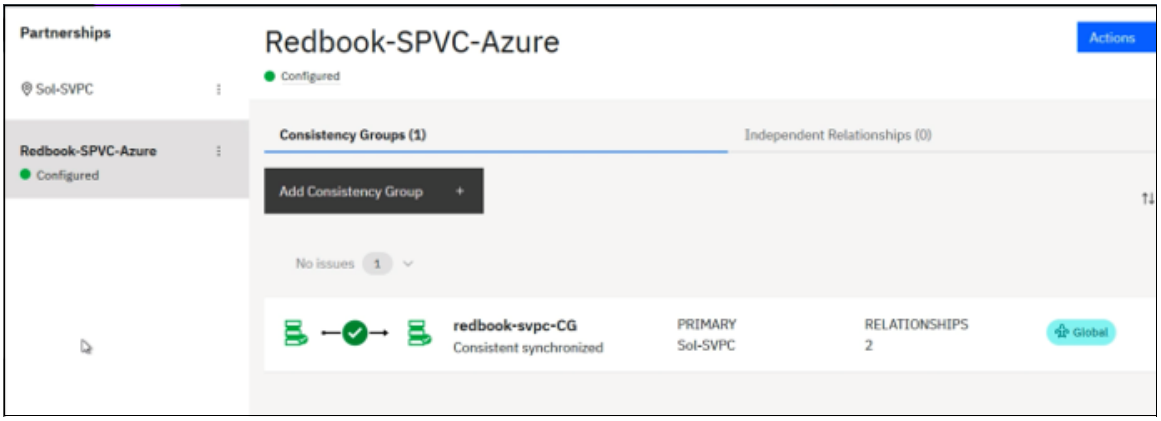


Figure 36 Copy status displayed as consistent synchronized

13. Add the target volumes (`Sol-SVCP-target0` and `Sol-SVPC-Traget1`) to the volume group by logging in to the `Redbook-SVCP-Azure` (Site B) storage. Select **Volumes** → **Volume Group** → **Group Actions**. In the drop-down menu, select **Add volume**. Select the two volumes: **Sol-SVPC-target0** and **Sol-SVPC-target1**. Click **Add Volumes**.

    Ensure that the backup policy is assigned to the volume group for the scheduled Safeguarded Copy backup of the volumes (see Figure 37).

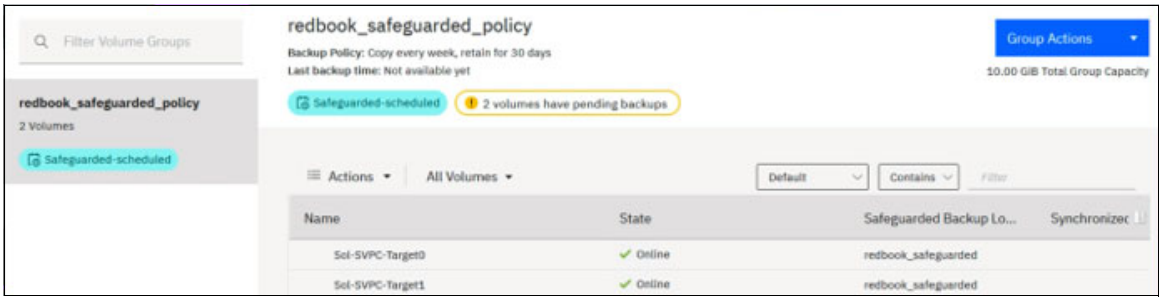


Figure 37 Volumes added to volume group

14. Log in to the IBM Copy Service Manager by using the `csmadmin` user and password. Select **Session** and you can see the newly created session in IBM Copy Services Manager. The `Redbook-Safeguarded-Policy` session was used in our lab setup (see Figure 38).

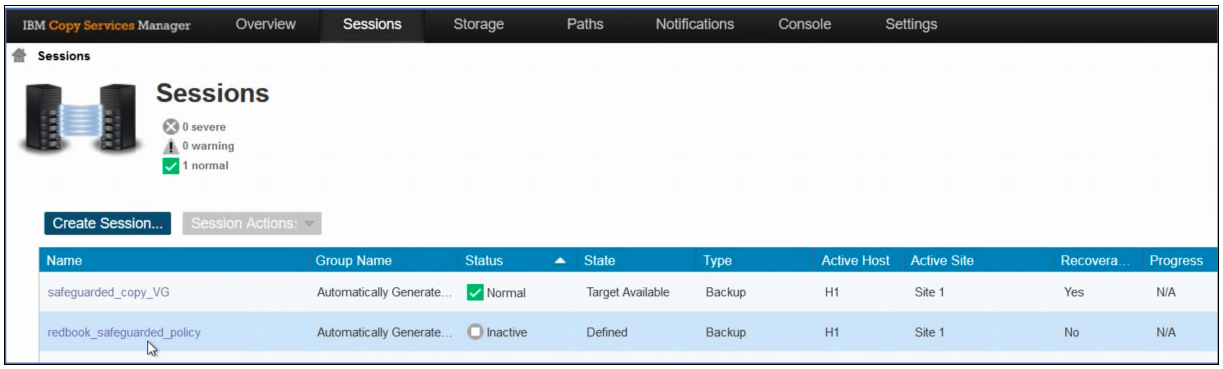


Figure 38 Session automatically discovered in IBM Copy Services Manager

15. Select **Redbook-Safeguarded-Policy** and then, select **Session Action** → **Commands** → **Backup** → **Retention days (1)**. Click **Yes**. The backup is created (see Figure 39).

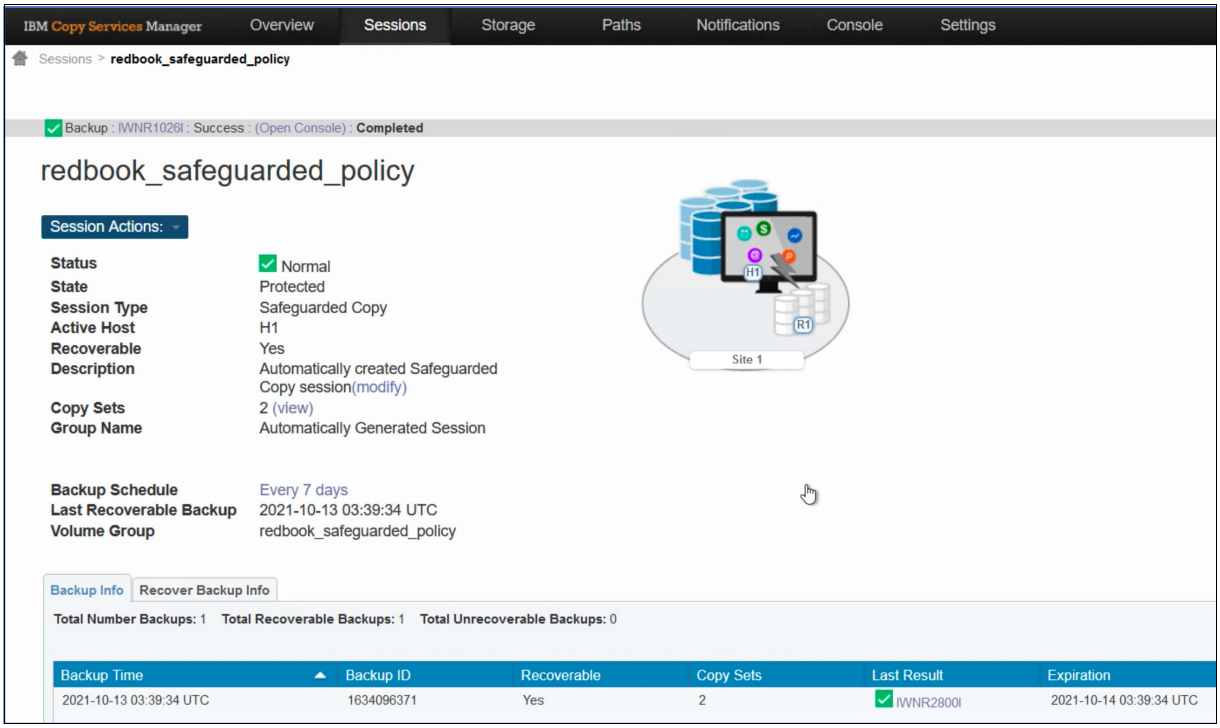


Figure 39 Safeguarded copy backup created

16. Log in to the SV4PC Storage and select **Pools**. Click the Safeguarded Pools and verify that the backup volumes were created (see Figure 40).

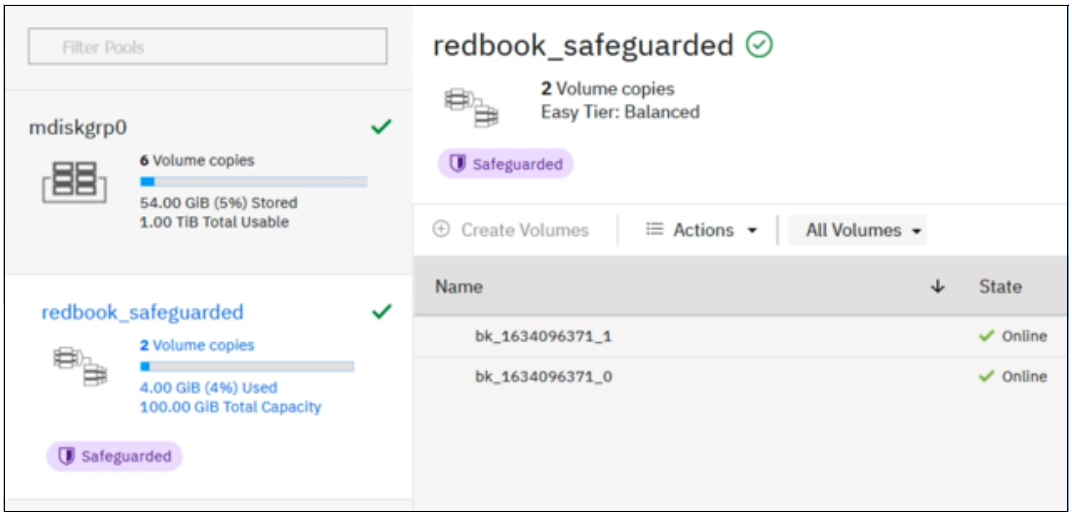


Figure 40 Safeguarded copy backup volumes created

Similar to how you can recover the volumes, after the backup is completed, log in to IBM Copy Services Manager and select **Session Actions** → **Commands** → **Recover Backup**. Select **backup ID** and click **Yes**.

17. Click the Recover backup tab and check the status of the recovery, as shown in Figure 41.

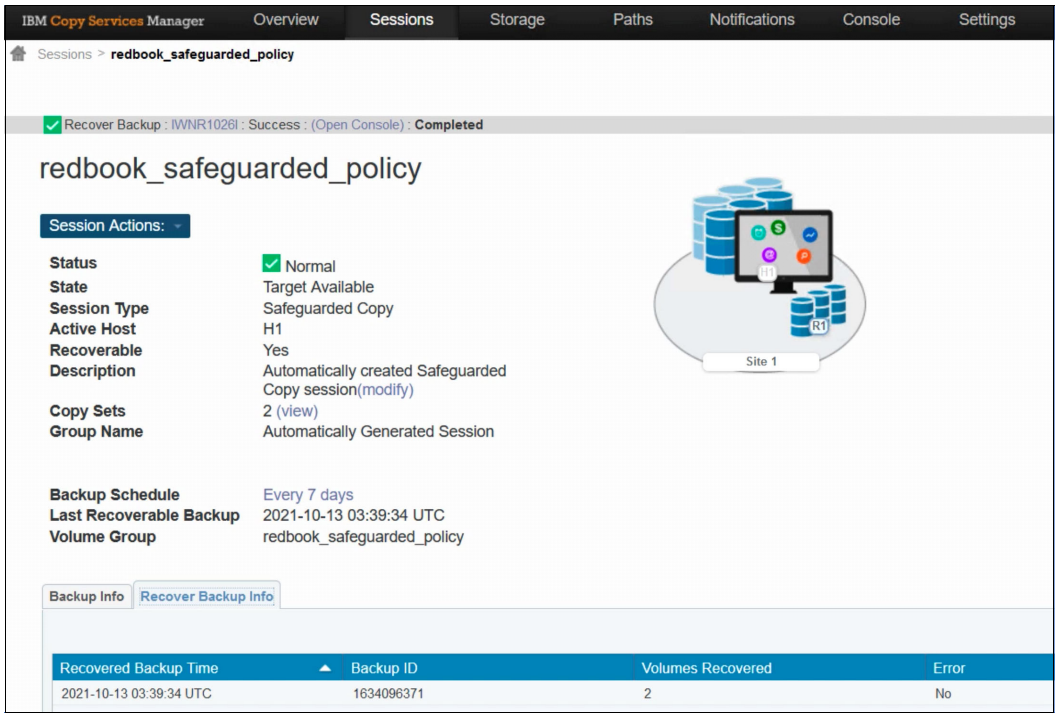


Figure 41 Recover backup info volume information

18. Log in to the SV4PC Storage and select **Pools**. Click **Safeguarded Pool** and check that the recover volumes were created in the pool, as shown in Figure 42.

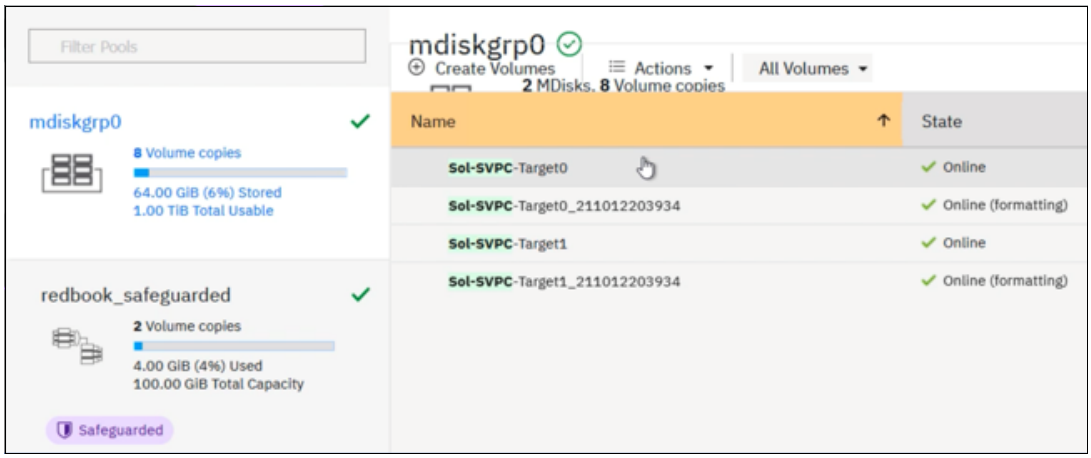


Figure 42 Recovered volume information

19. To map the recovered targets to the recovery host, log in to the SV4PC storage (Site B). Click **Hosts** and then, select **Volumes by hosts and Clusters**.

20. Select **Host Restore-VM** → **Host Actions** → **Modify volume mapping**. Click **Add Volume mapping**. Select the recovered volume and then, click **Next**. Click **Map Volumes** (see Figure 43).

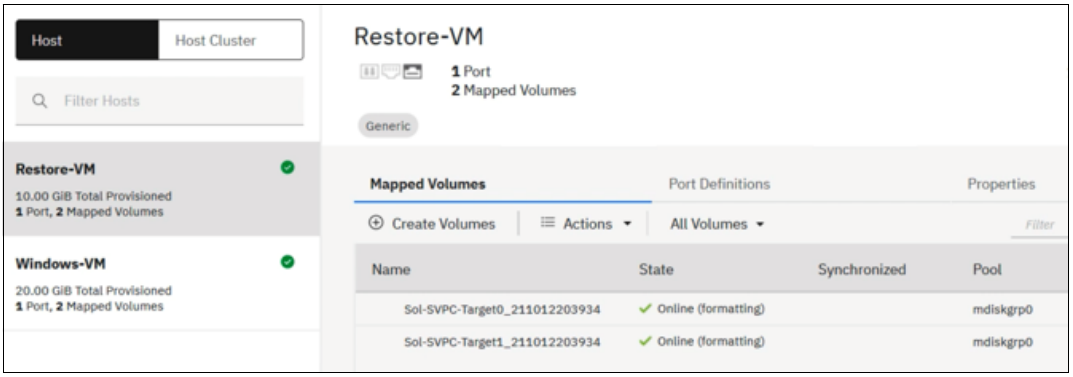


Figure 43 Mapped recovered target volumes to host

21. Log in to the target VM; that is, Restore-VM (Windows 2019 DC Host). Open Computer management and select **Disk management** → **Rescan Disks**. Then, select the disk and right-click and select **Online**, as shown in Figure 44.

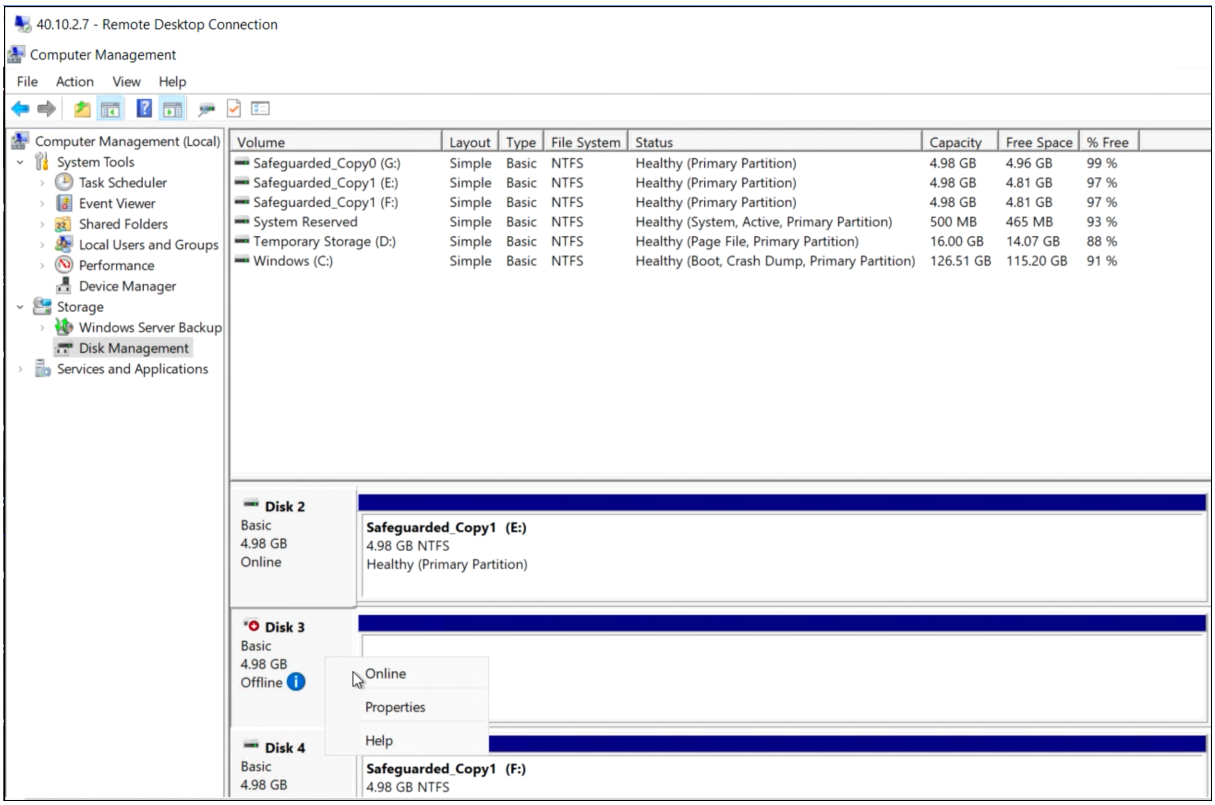


Figure 44 Restore VM Volume information for sample data

22. Check the status of the test folder that is available in the recovered volumes, as shown in Figure 45.

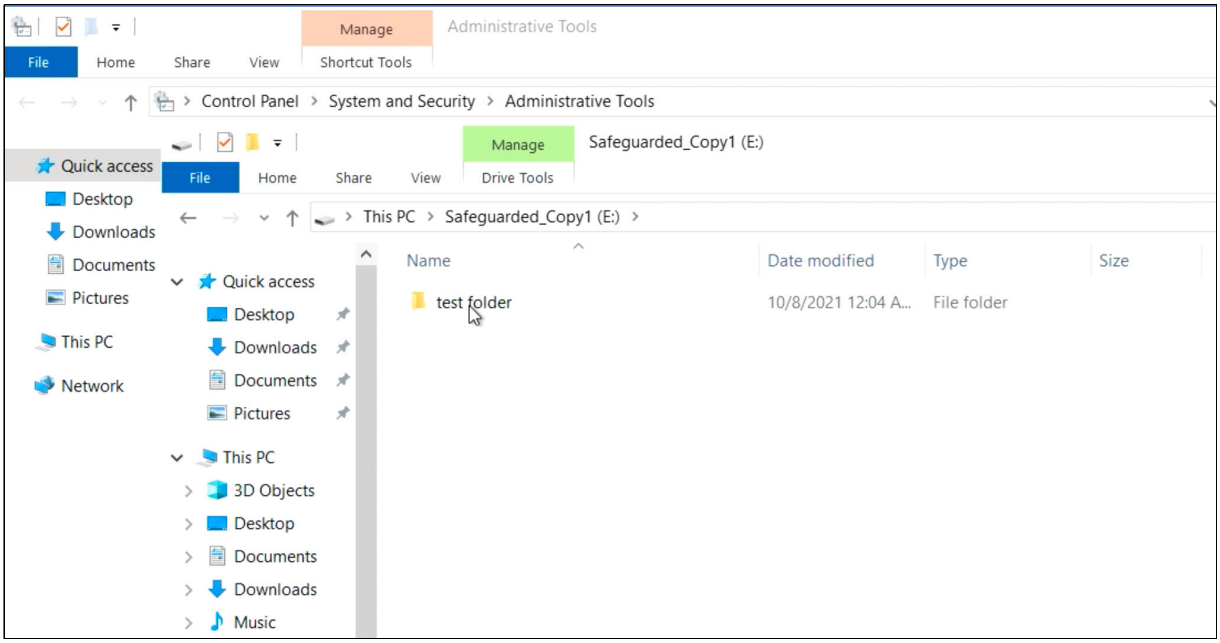


Figure 45 Sample data available on the restored volume

This demonstration showed how to create a Safeguarded Copy solution for the cloud scenario for the IBM SV4PC storage in Azure. The Safeguarded Copy function was performed on the replicated Spectrum Virtualize instance, which is airgap isolated from the instance that is running the primary workload.

Acknowledgments

The author wishes to thank the following people for their contributions to this project:

Hemant Kantak
Hemanand Gadgil
IBM, Solution Architects

Michelle Tidwell
Program Director | Global Offering Manager, Spectrum Virtualize, IBM

Jackson Shea
Senior Certified IT Specialist (LVL2)

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.

FlashCopy®
IBM®
IBM Cloud®
IBM Cloud Satellite™
IBM FlashCore®
IBM FlashSystem®
IBM Spectrum®
Passport Advantage®
Redbooks (logo) ®
Satellite™
Storwize®

The following terms are trademarks of other companies:

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

Ansible, OpenShift, Red Hat, are trademarks or registered trademarks of Red Hat, Inc. or its subsidiaries in the United States and other countries.

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.

January 2022

Please recycle

ISBN 0738460346

REDP-5674-00