Hewlett Packard Enterprise

HPE Reference Configuration for Enterprise Active Archive Backup to HPE Scalable Object Storage with Scality RING

Solution overview and configuration details for Enterprise Backup using HPE Apollo 4000 Systems

Reference Architecture

Contents

Executive summary

Explosive growth in unstructured data continues to put pressure on IT administrators to optimize data-storage practices, control storage IT spending, and still meet backup SLAs. New technologies, such as high-resolution cameras, medical imaging, seismic data, and more are multiplying that growth. Backup costs are skyrocketing, but much of the data is infrequently accessed. Maintaining this data on primary NAS/SAN storage is very expensive and leads to missed backup windows.

The architecture described in this paper provides a financially attractive alternative to traditional backup methodologies that store backup data on tape, on purpose-built backup appliances, or even on primary storage tiers. Massively scalable object storage allows customers to build on-premises private clouds that can store large amounts of backup data at costs comparable to public cloud storage (including hardware and maintenance). This object storage approach allows enterprises to consolidate multiple use cases into a single large data repository, with data from enterprise backups being only one type of data that can be stored.

HPE Scalable Object Storage with Scality RING™, a software-defined storage platform, running on HPE Apollo 4000 storage servers significantly lowers the cost of long-term, online backup storage. It natively interfaces with industry-standard enterprise backup software to move data off more expensive storage tiers, freeing those resources. Leveraging a core object-based technology, this solution provides a lower infrastructure cost and a significantly higher level of scalability than traditional backup storage systems. This solution is complementary to existing environments and can be easily integrated into existing workflows. As an added benefit, it offers a geographically distributed model and therefore contributes to business continuity planning.

Scality RING scales as a single uniform system, from hundreds of terabytes to petabytes and exabytes, so you never worry about a limit on capacity expansion or creating multiple data silos. Unlike physical tape, with Scality RING your data is automatically made durable, and backups are always online for access with high throughput and low latency. Unlike public clouds, Scality RING lets you budget and control costs with no hidden fees for accessing your data. HPE Scalable Object Storage with Scality RING gives you the performance and protection of an on-premises solution with the flexibility and economics of the cloud.

Scality has certified the file system and S3 Connectors with dozens of the most popular business applications, which enable a variety of uses for HPE Scalable Object Storage with Scality RING. This paper focuses on using Scality RING as the primary target for backups, and as the archive target for long-term storage of backups.

Target audience: This Reference Configuration describes the HPE Scalable Object Storage with Scality RING solution, with information about configuring enterprise backup applications and deploying HPE Apollo 4000 storage servers. We assume that readers of this document are familiar with backup application configuration and administration, and with HPE StoreOnce Systems (HPE StoreOnce) administration and use.

This document is intended for those who maintain, evaluate, or design backup and storage systems, including solution architects, database and backup administrators, and others wishing to learn more about how the HPE Scalable Object Storage with Scality RING solution can significantly lower infrastructure costs and increase scalability. This document focuses on the configuration required to attach enterprise backup software to HPE Scalable Object Storage with Scality RING, and therefore assumes the object storage cluster and the HPE StoreOnce are already installed and configured.

This white paper describes a project developed by Hewlett Packard Enterprise in December 2017.

Disclaimer: Products sold prior to the separation of Hewlett-Packard Company into Hewlett Packard Enterprise Company and HP Inc. on November 1, 2015 may have a product name and model number that differ from current models.

Introduction

We live in a world where everything computes—thanks to constant connectivity, easy access to massive computational power, exponential increases in data, and even human-machine interaction. These capabilities are pervasive; they are upending industries and creating new possibilities around the world at a pace we've never seen. This disruption and continuous innovation is our new normal.

The data landscape is rapidly evolving and growing. Analytics used to be limited to historical analysis of business data, but 90% of the world's data was created in the past two years. This tremendous growth is from new data sources, machines, and IoT, as well as human-generated data, such as social media, videos, and smart phone camera imagery. Analyzing this data together creates the opportunity for developing integrated business intelligence.

We are now in the age of Moore's Law for digital storage: data more than doubles every year. The core of the challenge is simply the amount and growth of data, with IDC predicting that the "data universe" will reach 163 zettabytes by 2025.[1] This data is coming from 8 billion people and 30 billion devices, running 10 million different applications. According to the Economist Intelligence Unit (2013), it is estimated that 80% of the data is unstructured, meaning the data has no predefined data model.[2]

Of particular relevance is that large organizations will have petabytes of data to manage, of which the majority will be static and unstructured. Traditional storage can have difficulties meeting performance requirements at that scale since both management and availability become far more challenging. In addition, storage lifecycle expectations are often longer at scale, so that the affordability of storing data becomes even more acute, especially for static and unstructured data.

Hewlett Packard Enterprise addresses this exponential growth of unstructured data and difficult-to-manage costs using Scalable Object Storage with Scality RING. Scality RING object storage extends the life of your primary NAS or SAN storage by enabling you to offload long-term storage of backup data from higher cost storage systems and store the data in the most space-efficient manner. Doing so enables you to control costs with on-premises, software-defined storage with the added flexibility for expansion to include hybrid-cloud configurations.

The data stored by most enterprises can be generally described as falling into two broad categories. Some data is transactional, meaning it is being actively used, updated, and modified. Other data is largely static, being inactive and perhaps immutable, such as surveillance video, medical imaging and records, genomics data, backups of email and other files, seismic data, financial transaction history, or IoT data. Most of the static data kept by an organization can be managed like objects, meaning the data is complete, will not be modified, and is ready to be stored or archived. Previously, this type of data would be sent to an archive, or offloaded to tape. Using HPE Scalable Object Storage with Scality RING, this data can be stored more economically than with conventional storage, while preserving online access at the speed of a modern storage system.

Due to regulatory requirements, such as Dodd-Frank legislation in the financial industry and the EU Data Protection Regulations in healthcare, data must be stored for longer periods. Backing up such data becomes more difficult as the amount increases. Yet backup windows are shrinking, and data is often used 24x7. Traditional storage approaches are very expensive, do not scale easily, and often maintain long-term copies of backup data on tier-1 storage. Using offline or tape archives is often not an option for many enterprises due to compliance and security demands requiring readily accessible data on-premises. A solution to these challenges is HPE Scalable Object Storage with Scality RING. Backup data stored in a Scality RING is always online and available, allowing immediate restores without additional overhead, even during planned and unplanned system maintenance.

HPE Scalable Object Storage with Scality RING running on HPE Apollo 4000 storage servers provides a reliable, high-performance, and cost-effective backup and archive solution that scales to meet the unique application requirements of supported ISVs, such as Commvault, IBM Spectrum Protect, and Veritas NetBackup. This solution enables worry-free capacity expansion when the backup and archive data grows, since storage is managed by the Scality RING software-defined storage layer and only indirectly tied to external storage systems themselves.

Unlike conventional NAS storage systems, HPE Scalable Object Storage with Scality RING running on the storage-density-optimized HPE Apollo 4000 storage servers enables high availability and 14 nines of data durability, with a disk-based solution at a cost equivalent to tape. Moreover, this solution has the added benefit that data retrieval is much faster and far easier than from physical tape or public cloud.

HPE Scalable Object Storage with Scality RING provides always online access to your data at cloud-scale pricing, including the following features:

- Control costs with on-premises software-defined storage built on reliable HPE Apollo 4000 storage server platforms.
- Scale virtually without limits—linear performance in less space with extreme data availability.
- Simplicity in management with graphical and command line tools along with the HPE Integrated Lights-Out (iLO) feature.

[1] *Data Age 2025: The Evolution of Data to Life-Critical: Don't Focus on Big Data; Focus on the Data That's Big*. https://www.seagate.com/files/www-content/our-story/trends/files/Seagate-WP-DataAge2025-March-2017.pdf. IDC White Paper, sponsored by Seagate, Data Age 2025, April 2017.

[2] "Data are growing not just in volume but variety too. It is now estimated that 80% of data are unstructured, meaning they have no predefined data model. This presents new kinds of data management challenges: a plan by the city of Chicago to open its data to software developers requires cleaning up 10 billion lines of unstructured data." http://economist.com/news/united-states/21576694-cities-are-finding-useful-ways-handling-torrent-data-numbers.

- Flexibility to access your data at petabyte scale via multiple protocols including NFS, SMB, and S3 interfaces.
- Migration-free storage solution with built-in data integrity requires no additional backup to protect your data.
- High resilience with low overhead, even using multisite configurations

Economics of the solution

Many solutions combine an object-storage system with a standard tape library for additional storage and for offsite copies of critical data. HPE Scalable Object Storage with Scality RING has all of the data functions required for data ingest and protection, providing the benefits of disk storage at the cost of tape. Scality RING object storage allows you to replace tape archives with a petabyte-scale disk solution with the potential to transform your archives from a cost center into a profit center.

Using Scality RING object storage to back up data to an enterprise active archive allows you to disrupt storage economics, not your business. Scality RING object storage includes built-in data integrity, so no additional backup is needed and allows instant access to archived data with high resilience, including site resiliency if configured as a geographically dispersed RING. This reduces management effort and lowers overhead. Scality RING scales as a single uniform system, from petabytes to exabytes, with on-premises deployment costs competitive to tape and public cloud.

Scality RING object storage is a 100% migration-free storage solution: once in the RING, no more migrations or backups are necessary to protect your data. Scality RING object storage allows you to store inactive and immutable data in a cost-optimized storage tier, which improves storage utilization and lowers your tier-1 storage needs. You can cap new expenditures for primary storage and re-allocate savings to close budget gaps. Scality RING object storage enables the retirement of older technologies; thereby, reducing power, cooling, floor space, and administrative costs. With Scality RING object storage, there are no hidden data access or migration fees, as may be incurred with public-cloud providers.

HPE Scalable Object Storage with Scality RING provides always-online, on-premises access to your data at cloud-scale pricing. Primary storage on NAS/SAN is often unnecessarily over-provisioned due to inactive and/or immutable data residing on the tier-1 storage. In many cases, over 50% of the data contained on NAS/SAN systems is accessed infrequently, yet stored on the same tier of primary storage as active data.[3] The total cost of ownership (TCO) of NAS/SAN storage is heavily impacted by the cost of backing up inactive and immutable data, along with transactional data in active use.

Offloading inactive and immutable data from higher cost storage to Scality RING object storage reduces the amount of primary data to be backed up and pays dividends in three ways:

- The amount of primary storage capacity required is reduced, since inactive data is no longer being maintained on your tier-1 storage.
- The capacity of the backup system can be reduced, since inactive data has been offloaded to Scality where data protection is built-in and no additional backup is needed.
- Management time and backup windows are both reduced, resulting in cost savings.

Some IT organizations are evaluating whether it makes sense to move aspects of their managed operations to environments hosted by a Cloud Service Provider. While relevant to the subject of this paper, the analysis required to objectively compare TCO for on-premises environments and cloud-hosted environments can be complex. Therefore, any detailed TCO analysis between these environments is largely outside the scope of this document.

[3] For more information, go to *What is Archive Anyway*? at https://storageswiss.com/2015/10/16/what-is-archive-anyway

Solution overview

The Scality RING software automatically manages storage in a space-efficient way and can be configured for multiple levels of data durability, using erasure coding and replication. When objects are stored using erasure coding, the Scality algorithm encodes the data for durability and distribution across the RING. Scality RING has the flexibility to be configured as a single-site, on-premises cluster, or a multi-site geo-distributed RING with native geographically dispersed clustering. Whether single-site or geo-dispersed, flexible "failure domains" can be configured to tolerate the loss of physical or logical components. This produces native data protection in a distributed architecture with no single point of failure, resulting in a self-healing RING that protects data from equipment failures, network outages, and even site-wide failures and disasters.

Scality's policy-based data protection yields extreme data durability, which dramatically reduces the risk of data loss and enables you to store more for less, with the data still fully accessible. There is no downtime from faults, upgrades, or hardware refreshes since the Scality RING can provide 14 nines of data durability. Maintaining business continuity is much easier with continuous access to your data.

Manage your data at scale with true enterprise-grade HPE industry-standard server monitoring and management tools designed for IT generalists. The Scality RING's ability to transparently manage planned and unplanned events results in lower operational expenses by reducing the manpower required to manage petabytes of data. HPE Scalable Object Storage with Scality RING gives you the flexibility to control costs using software-defined object storage built on reliable HPE platforms for on-premises deployments, achieving cloud economics, scalability, and giving you full control of the data.

HPE Scalable Object Storage with Scality RING can be used in many cases as a primary backup target. It is also ideal for long-term retention of backups, where the primary short-term backup target might be the HPE StoreOnce Systems (HPE StoreOnce). In typical object storage deployments, a single HPE-Scality RING cluster can archive backups, and provide other storage use cases where objects make sense and capacity/bandwidth considerations are practical.

For example, service providers and web application providers can host scale-out object storage as a service for consumers, small-to-medium businesses, and enterprise customers. Media and entertainment companies can use HPE Scalable Object Storage for Nearline archives, as a staging area for post-production workflows, as a long-term archive for completed video production projects, and as the content origin for web streaming of education or consumer videos. Government, medical, and university research organizations can use object storage for long-term archives of intelligence information, medical imaging and records, or other research data. Large enterprises such as oil and gas companies, financial institutions, life sciences organizations or manufacturing companies can use scalable object storage for financial transaction compliance archives, CCTV archives for surveillance systems, or as active archives for high performance computing (HPC) data from seismic or genomics research.

While the possible uses and applications of HPE Scalable Object Storage with Scality RING are many and varied, this paper focuses on the following two scenarios:

- Use case 1: Backing up directly to HPE Scalable Object Storage with Scality RING
- Use case 2: Backing up to an HPE StoreOnce with copy to HPE Scalable Object Storage with Scality RING

The industry-leading backup applications discussed in this paper are Commvault, IBM Spectrum Protect, and Veritas NetBackup, listed here and throughout this paper in alphabetical order by company name.

Figure 1 is a high-level sketch of the configuration used with each backup application described in this paper. This diagram illustrates a typical configuration.

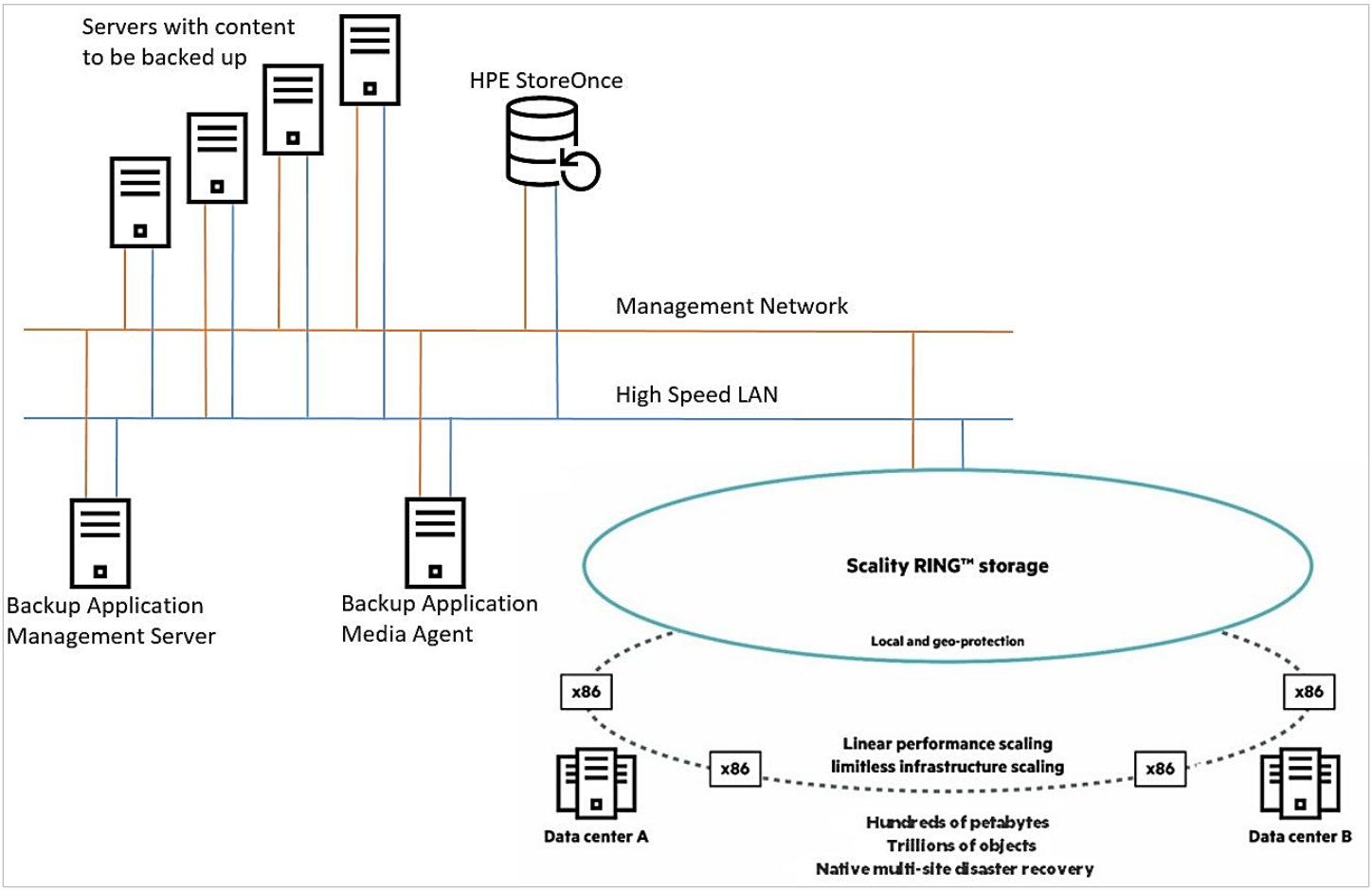

Figure 1. Architecture diagram for HPE Scalable Object Storage with Scality RING on HPE Apollo 4000 storage servers and backup applications

Solution components

This solution has been tested with Commvault, IBM Spectrum Protect, and Veritas NetBackup. Configuration instructions and details specific to each application are included in the appendices of this paper. Please refer to the documentation from each backup application's vendor for additional detail and any best practices associated with their use of HPE Scalable Object Storage with Scality RING and the Scality S3 Connector.

HPE Scalable Object Storage with Scality RING

The HPE Scalable Object Storage with Scality RING is a scale-out, software-defined storage solution (SDS) providing petabyte-scale data storage designed to interoperate in modern software-defined data centers (SDDC). The RING software creates virtually unbounded scale-out storage to consolidate and protect data from multiple applications and workloads, including both file and object applications. The RING software provides a set of intelligent services for data access, data protection, and systems management. The top layer of data access services offers native file and S3-compatible cloud-object storage interfaces for applications.

Large distributed systems depend on fast and efficient routing of requests among the member nodes. At the heart of the RING storage layer is a scalable, distributed key-value object store based on Chord, a second-generation peer-to-peer routing protocol designed at MIT. The protocol is highly responsive to changes in system topology, such that these changes do not require broadcasting to all nodes but only to a few relevant nodes. This enables the protocol to work efficiently in very large clusters. Scality has augmented the basic Chord protocol to enable higher levels of data durability, improved performance, self-healing, efficient geo-scale deployment, and simplified management.

For data protection, the RING provides customizable availability and failure domains. Customers can configure the data-protection policy at the object level, with replication of up to five copies, or erasure coding to provide as much as 14 nines of durability with low overhead for larger objects. Data protection options include geo-redundancy, providing additional tolerance of multiple disk, server, rack, and even site communication failures or disaster scenarios.

The RING's advanced routing capabilities, configurable data management, and software-defined architecture provide full system availability and uptime during planned and unplanned events, including hardware failures, hardware refreshes, capacity upgrades, and software upgrades. Managing and monitoring the RING is enabled through a graphical web portal called the RING Supervisor, through a scriptable command-line interface (CLI), and monitoring/alerting from SNMP-based consoles. The RING is designed to be self-managing and autonomous, freeing administrators to work on other value-added tasks.

The RING software is deployed as a distributed system on a minimum cluster of six storage servers. This system can be seamlessly expanded online to thousands of physical storage servers as the need for storage capacity grows. The HPE Apollo 4000 storage servers provide a combination of hard disk drives (HDDs) for RING data, and solid-state disks (SSDs) or non-volatile memory (NVRAM) for RING metadata. Scality RING Connector services can be run directly on storage nodes for maximum efficiency, or on external gateway servers for flexibility.

HPE Apollo 4000 storage servers

The HPE Apollo 4000 storage-density-optimized servers are purpose-built as object-storage platforms and for big data. The power and flexibility of the HPE Apollo 4000 platform enables a robust and scalable object storage solution that with Scality RING provides linear scale-out as a single protected system across multiple sites and thousands of servers. The HPE Apollo systems can be configured to serve as both storage nodes and connector nodes in Scality RING clusters.

The HPE Apollo 4000 platforms are available in standard rack unit sizes: the HPE Apollo 4510 Gen10 system in 4U, and the HPE Apollo 4200 Gen9 server in 2U. Both systems leverage the modular and efficient Apollo chassis infrastructure to provide leading storage density and operating efficiency. The HPE Apollo 4000 storage servers provide configuration flexibility to optimize for capacity, throughput, and responsiveness. The systems are designed to maintain availability, data recovery, and support serviceability. Hot-plug critical components (disk drives, nodes, fans, and power supplies) provide serviceability at every level.

HPE Apollo 4000 systems include the HPE Integrated Lights-Out (HPE iLO) management capability, allowing secure management and monitoring of servers from practically anywhere. HPE Apollo 4000 systems integrate with HPE OneView for automating the management of IT infrastructure. The HPE Smart Array controllers are available to provide services such as Secure Encryption with FIPS 140-2 certification. This enterprise-class solution uses dedicated encryption hardware and is verified to have a low impact on input/output operations per second (IOPS) in addition to operating system transparency.[4]

[4] For more information, refer to *HPE Scalable Object Storage with Scality RING on HPE Apollo 4510 Gen10* white paper at https://www.hpe.com/h20195/V2/Getdocument.aspx?docname=a00026022enw

Commvault

Commvault is an enterprise-class, data-protection application that is scalable from small-to-medium businesses to global enterprises.[5] Commvault software combines data protection and recovery into a single virtual data repository and eliminates the separate data repositories associated with traditional backup and archive products. Commvault provides a unified view of all managed data regardless of residence. Commvault software enables organizations to protect data across multiple storage tiers to reduce costs and improve efficiencies. This enables users to access and restore data selectively, without the need for a complete recovery.

Commvault software provides a powerful set of storage management tools that help move and manage critical data. These tools enable users to store and retrieve data associated with computer systems in the enterprise. The system consists of integrated software modules, which can be grouped together in a CommCell configuration. Each CommCell configuration consists of the following main components:

- One CommCell server
- One or more clients running an agent, such as the OnePass Agent, that perform backup, archive, and restore operations
- One or more media agents

Once installed and configured, these CommCell elements can be controlled and monitored from a single unified CommCell Console.

IBM Spectrum Protect

IBM Spectrum Protect is a highly scalable and flexible application providing fully managed backup and archive solutions.[6] The Spectrum Protect approach to storage management is complex, and the product differs from other backup applications in several significant ways, including its client/server architecture, progressive incremental backup methodology, and unique data and storage policy objects. Moreover, Spectrum Protect catalogs and controls data objects instead of simply managing storage media. Spectrum Protect data objects include the following:

- Sub-file components, files, directories, or raw logical volumes
- Blocks of client data that need to be archived for a fixed amount of time
- Tables or records from database applications

By default, Spectrum Protect performs a special kind of backup called a *Progressive Incremental* or an *Incremental Forever* backup. This Progressive Incremental backup combines the benefits of an incremental backup with the restore benefits of a differential backup. Files are backed up incrementally to reduce network traffic, while recovery media is consolidated to provide better restore performance. All metadata is stored in the Spectrum Protect database, and all object data is stored in the assigned Spectrum Protect storage media device.

A Spectrum Protect environment consists of three basic types of resources: clients, data, and rules. The Spectrum Protect client systems generate the data, and the rules specify how that data will be managed. For example, in the case of backups, rules define how many versions of a file should be kept and where they should be stored. These Spectrum Protect *Policies* define the relationships between the three basic resource types described above. Spectrum Protect Backup and Archive Policies can be relatively simple or incredibly complex, depending on your data needs.

To store and manage data objects on different types of storage media and devices, Spectrum Protect implements several logical entities to classify the available physical hardware storage. The hardware is assigned to a Spectrum Protect *Device Class*, which is then correlated to a Storage Pool. At the heart of the Spectrum Protect environment is the *Storage Pool*. Storage Pools are the central element of the Spectrum Protect storage management environment because they provide the link between the Spectrum Protect Client Data and the underlying Storage Objects.

Spectrum Protect organizes Storage Pools into one or more hierarchical structures, called *Policies*. Each storage hierarchy can span multiple Spectrum Protect Server instances. These storage policies are then used to migrate data objects automatically from one Storage Pool to another. Cloud-Container Storage Pools, using S3-Compliant object storage, are one new type of Storage Pool that Spectrum Protect now supports.

[5] As of 2016, Commvault dropped the Simpana brand.
[6] Beginning with Version 7.1.3, IBM Tivoli Storage Manager (TSM) was rebranded as IBM Spectrum Protect.

Veritas NetBackup

Veritas NetBackup is a leading enterprise software suite for backup/archival solutions that is built to protect large and demanding enterprise environments. NetBackup provides a holistic backup and recovery solution optimized for data protection that can scale nicely with object storage solutions. NetBackup has a three-tier architecture that consists of the following components:

- **Master Server**—maintains a database with information about backup images, system configurations, and available backup resources. The Master Server is responsible for initiating backups as scheduled by any configured backup policies, and also for scheduling and allocating the required resources to complete each job.
- **Media Server**—dedicated to reads and writes of backup and restore data between clients and designated backup media. The Media Server owns one or more backup devices. In the case of this solution, the "backup device" is the Scality RING object store accessed by the Media Server. Backup resources can be partitioned and shared between multiple Media Servers.
- **Clients**—Systems where the data to be protected resides.

NetBackup Cloud Storage enables backup and restore operations from cloud vendors and is integrated with Veritas OpenStorage. The features and functionality that NetBackup Cloud Storage provides include the following:

- A Cloud Storage Server Configuration wizard to set up cloud storage and provision the storage.
- NetBackup Cloud Storage Encryption, which optionally encrypts data inline before it is sent to the cloud. The encryption feature uses AES 256 cipher feedback mode encryption.
- NetBackup Cloud Storage throttling to control the data transfer rates between the network and the cloud. Throttling values are set on a per NetBackup media server basis. Throttling can specify different bandwidth for both read and write operations. Network bandwidth can be specified as a percent of total bandwidth and can be set per block of time. Throttling also controls the maximum number of connections to the cloud service provider at any given time.

Details are available in the *Veritas NetBackup Cloud Administrator's Guide*, veritas.com/support/en_US/article.000116367

Best practices and configuration guidance for the solution

Configuring HPE Apollo 4000 storage servers and HPE Scalable Object Storage with Scality RING and Scality S3 Connector

No special configuration of the HPE Scalable Object Storage with Scality RING is needed to use object storage with backup applications. The Scality RING is delivered from HPE as a fully functioning S3 target, ready to be used immediately with applications such as Commvault, IBM Spectrum Protect, and Veritas NetBackup.

The Scality RING is managed securely via a scriptable Python-based CLI or a web-based Supervisor GUI over HTTPS with password login access. The GUI provides customizable one-screen RING management and reporting, which includes storage provisioning, capacity monitoring and planning, connector control, RING key management, hardware health monitoring, and platform-specific reporting of HDD health from the HPE Apollo 4000 servers. The reporting functions include performance and resource graphs, as well as other statistics and metrics to help you manage the Scality RING resources.

In addition, HPE Integrated Lights-Out (iLO) provides the automated intelligence to maintain complete server control from anyplace. HPE iLO functions out-of-the-box without additional software installation, regardless of the server's state of operation, giving you complete access to your servers from any location via a web browser or the iLO Mobile App. Additional information on HPE iLO can be found at hpe.com/us/en/servers/integrated-lights-out-ilo.html

While Scality RING provides the flexibility to support single-site and geo-dispersed configurations with nodes in multiples of six, testing for this paper was conducted on a single-site, six-node cluster of HPE Apollo 4000 storage servers and HPE Scalable Object Storage with Scality RING. This configuration represents a basic out-of-the-box setup.

When configuring the target settings in your backup application, you must specify the path to the object store you wish to use and provide the bucket name, access key, and secret key. The path to the object store is specified using a URL or IP address.

Using CloudBerry Explorer to create and view object storage buckets

The Amazon S3 API stores objects in containers called *buckets*. When using HPE Scalable Object Storage and the Scality S3 Connector with Commvault and IBM Spectrum Protect, you must specify a bucket name that already exists in Scality object storage. Veritas NetBackup creates the buckets during configuration and setup. However, when using NetBackup with HPE StoreOnce Cloud Bank Storage (described later in this paper), HPE StoreOnce requires that the name of an existing bucket be specified. None of the backup applications or appliances mentioned here include a client interface for creating or viewing buckets on Scality; the buckets must be created using a separate application.

For an example configuration scenario, refer to Appendix A: Cloudberry Explorer configuration details on page 19.

Data sets used in testing

Testing for both Commvault and Veritas NetBackup used the data sets described in Table 1. The characteristics of these data sets were chosen to represent a wide range of environments, so there is a large variation in the size, number, and type of files contained in each set. Data set 1, being a collection of various document files, is compressible. Data sets 2, 3, and 4 are not compressible due to the nature of the files contained in them. The video files in data set 2 are already compressed, as are the zip files in data set 3 and the ISO images in data set 4. Data set 5, consisting of binary files, is highly compressible and has a higher deduplication ratio than the other data sets. The varying amount of compressibility and the amount of deduplication of each data set impacts the performance results, as shown in the tables in Overview of backup and restore performance below. For example, a group of files that is highly compressible and has a high deduplication ratio, such as data set 5, may consume less network bandwidth and transfer time than expected when compared to a non-compressible data set with little deduplication that is half the size, like data set 3. The effect is most pronounced in operations where the data sets have been deduplicated by the HPE StoreOnce.

Table 1. Data sets used in testing Commvault and Veritas NetBackup

Data set	Number of files	Total size	Range	Description
1	2,188	1.99 GB	1 KB – 302 MB	Document files of various types (pptx, xlsx, docx, pdf, txt, etc.)
2	40	6.58 GB	1 MB – 782 MB	Video files from a surveillance system
3	26	80.3 GB	105 MB – 18 GB	Collection of audio files in .zip format
4	43	91 GB	1.5 MB – 6.5 GB	Various OS ISO images
5	118,104	153 GB	4 KB – 8 MB	Binary files

Overview of backup and restore performance

The performance of cloud-based object storage is heavily dependent on the network connection between the backup application server and the HPE Apollo/Scality S3 Connectors. Performance is also affected by the workload being sent to and processed by the Scality RING. If the RING is hosting more than just backup operations and the network connection is extremely busy, backup and restore performance could be impacted.

This paper is not intended to assess backup performance of the various applications tested with respect to each other. Rather, the purpose is to demonstrate that the applications listed work smoothly with Scality RING storage and to demonstrate the proper configuration steps in each application to use HPE Scalable Object Storage with Scality RING. While performance was not a main focus of this paper, various sampling was done to determine that backup performance is adequate. In all cases, backup and restore performance was as expected; using Scality RING object storage with the S3 Connector did not differ appreciably from the performance normally seen with other backup appliances in a similar configuration.

As is to be expected, performance observed during this testing was dependent on the size and characteristics of the data being backed up or restored. For example, backup throughput (MB/s) for many small files was somewhat lower than for fewer files of a very large size. This is a common characteristic that is often observed with many other backup appliances and storage systems.

Our testing used a single 10 GbE connection between the backup servers and the S3 Connector. The observed single-stream throughput for a mixture of office files (as described in data set 1) was typically in the range of 100 – 125 MB/s. Throughput could be as high as 250 MB/s in certain configurations and with certain types of data. This is within the range of what was expected and can generally saturate a single 10 GbE link with 10 – 15 concurrent streams, or as few as 4 – 8 in certain circumstances.

There are several different approaches that can be implemented to achieve higher performance. For objects greater in size than about 600 KB, increasing processor performance with more cores or faster clock speeds has very little impact on performance. The single most effective way to increase performance is to improve network throughput. This can be done by bonding together multiple 10 GbE ports, using a faster network

(e.g., 40 GbE or a newer, faster network technology), or a combination of these factors. It is also desirable to enable multi-stream backups and to use more S3 Connectors. To achieve optimum performance for your configuration, HPE recommends implementing a combination of several of these options. Some of these configuration enhancements were implemented during our testing and found to improve performance as expected. Performance data is only reported for the minimal configuration used in this proof-of-concept.

In our testing only full backups were done; we did not test with incremental or synthetic full backups. Restores were of a full-image backup, which was written to a different location on the original server. Partial restores, using only selected files, were not tested.

All three backup applications tested provide the option of enabling encryption, compression, or both when writing data to cloud storage. When using a public cloud as the backup target, it is generally desirable to enable client-side encryption for data protection before it is sent to the cloud. Enabling compression on the client can also reduce the amount of data transmitted to the cloud, thus lowering costs for bandwidth utilization. The benefit of these options may not be as important when the backup target is an on-premises private cloud, such as HPE Scalable Object Storage with Scality RING. These options were exercised in our testing only to validate that they worked as expected with the Scality RING S3 Connector and HPE Scalable Object Storage. The features were indeed found to work acceptably in our configuration.

The tables below provide performance results for backup and restore operations directly to HPE Apollo 4000 storage servers and HPE Scalable Object Storage with Scality RING using the S3 Connector. The tables also show data for copy and restore operations in cases where the HPE StoreOnce was used as the primary backup target with Scality RING as the copy destination.

Note

These performance numbers are provided for general reference only and are not intended to be an indication of best performance. As stated above, there are a variety of configuration actions that can be taken to improve upon these performance numbers.

In the tables that follow, the performance metrics were derived from the information contained in the reporting features of the backup applications. No external means were used for measuring or validating performance. See Table 1 above for a description of the data sets used in these backup and restore operations.

Backup directly to Scality RING with only one S3 Connector

Table 2 lists the single-stream backup performance for each data set backing up to the Scality object store via a single S3 Connector. The configuration tested contained five connector nodes, in keeping with the minimum Scality RING configuration. The single-stream workloads used in this proof-of-concept did not saturate the 10 GbE link, so only one connector was needed. In a production environment, multiple connectors with a load balancer would improve performance significantly over what is shown in the table below.

Backups were launched manually, and new backups were launched after the previous backup completed. The client and media agent are the same for each of these backups, and the media agent is running Windows®. The network interface between the media agent and the Scality S3 Connector is a single 10 GbE connection. Performance across all backup applications tested was generally equivalent.

Table 2. Single-stream backups to Scality with one S3 Connector

Data set	Average elapsed time (mm:ss)	Estimated average throughput (KB/s)
1	0:54	109,879
2	1:02	164,841
3	11:09	131,883
4	12:14	136,279
5	23:20	121,934

Note

Performance in this case was limited by using only a single stream with the backup applications, not by the HPE Apollo storage servers or Scality RING. If multiple streams were used with all five of the available S3 Connectors and a network load balancer, performance would improve significantly over what is shown in the table above for a single stream with just one connector.

Restore

Table 3 lists the average restore times for each data set. The restore target was a location on the Windows client different from the source location.

Table 3. Single stream restore from Scality via the S3 Connector

Data set	Average restore time (mm:ss)
1	0:40
2	1:01
3	7:02
4	6:59
5	12:25

Backup to the HPE StoreOnce with copy to Scality RING

The applications tested handle copy operations in very different ways, described separately in this document. In order to perform the copy operation with Commvault, a Copy Policy must be in place, as described earlier. The copy operation can be scheduled or initiated manually and is managed by the Commvault media agent. When the auxiliary copy operation executes, the Commvault media agent reads the primary backup from the HPE StoreOnce NAS share. The deduplicated data is rehydrated as it is read from the HPE StoreOnce share. The media agent then writes the rehydrated data stream to the Scality object store via the S3 Connector. This behavior is considerably different from how copies are done using Veritas NetBackup and the Catalyst OST plugin for the HPE StoreOnce, and therefore cannot be compared with Catalyst backups and copies done with NetBackup.

Table 4 lists representative performance for each data set when the Commvault backup storage policy was set to use the HPE StoreOnce NAS share as the primary backup target and Scality object storage as the auxiliary copy target.

Table 4. Single-stream backup/copy performance to the HPE StoreOnce NAS share and Scality using Commvault

Data set	Primary backup to HPE StoreOnce NAS share		Auxiliary copy to Scality object storage	
	Average elapsed time (mm:ss)	Average throughput (KB/s)	Average elapsed time (mm:ss)	Average copy throughput (KB/s)
1	00:37	74,144	01:04	62,558
2	01:27	96,856	01:55	57,272
3	18:46	72,311	20:34	65,103
4	22:24	68,475	23:47	63,722
5	33:35	77,711	37:52	67,722

Of the three backup applications tested, only Veritas NetBackup integrates with the HPE StoreOnce OST plugin to support HPE StoreOnce Catalyst backup and copy operations. As described in Appendix D: Veritas NetBackup configuration details, a Storage Lifecycle Policy must be configured. When the Lifecycle Policy is executed, the backup is written to the HPE StoreOnce, using the built-in deduplication features of the HPE StoreOnce. The copy to HPE Cloud Bank Storage is initiated by the NetBackup media server, but managed by the HPE StoreOnce. A Catalyst Copy operation is performed to copy the Catalyst backup from the HPE StoreOnce to the HPE Cloud Bank Storage store on Scality RING. This behavior is very different from how copies are done with any other application, so performance of the NetBackup Catalyst backups and copy operations cannot be compared with the performance of any other application.

Table 5 lists representative performance for each data set when the NetBackup backup policy storage attribute was set to the Storage Lifecycle Policy: `StoreOnceStore-StoreOnce CloudBank`. Backups are directed to the HPE StoreOnce Catalyst store and duplication (copy) operations are directed to the HPE Cloud Bank Storage store, which is configured to write to the Scality RING S3 Connector.

Table 5. Single-stream backup/copy performance to the HPE StoreOnce Catalyst Store and HPE Cloud Bank Storage using Veritas NetBackup

Data set	Backup – HPE StoreOnce Catalyst store					Duplication (copy) – HPE Cloud Bank Storage store		
	NetBackup activity monitor		StoreOnce Catalyst data job			NetBackup activity monitor	StoreOnce Catalyst outbound copy jobs	
	Elapsed time (mm:ss)	Throughput (KB/s)	Data written	Write throughput	Data transferred	Elapsed time (mm:ss)	Copy throughput	Copy duration (mm:ss)
1	00:54	65,564	2.2 GB	76.9 MB/s	11.8 MB	02:05[7]	179.4 MB/s	00:13
2	01:42	82,910	7.1 GB	89.5 MB/s	42.1 MB	02:05[8]	110.5 MB/s	01:05
3	15:19	93,615	86.3 GB	96.4 MB/s	510.5 MB	12:02	123.4 MB/s	11:40
4	17:37	91,852	97.7 GB	94.5 MB/s	608.4 MB	11:32	147.8 MB/s	11:02
5	34:53	77,855	165.4 GB	80.0 MB/s	1.3 GB	02:42	1.3 GB/s	02:12

Restore

When data is restored from the HPE StoreOnce, the deduplicated data is rehydrated as it is read from the HPE StoreOnce to be written back to the client. When using Commvault, as with most other backup applications, restores from the secondary copy destination on Scality RING do not require rehydration during the restore operation since the data was already rehydrated when it was copied from the HPE StoreOnce to Scality.

Table 6 lists the typical time required for restore operations for each data set, restoring from the primary backup on the HPE StoreOnce. Restores were performed from the primary backup on the HPE StoreOnce NAS share, as well as from the auxiliary copy on the Scality object store. Only the restore operations from the primary backup on the HPE StoreOnce are listed in Table 6. The performance when restoring data from the auxiliary copy on Scality object storage is not listed here, but it was similar to the performance of restores from Scality, as shown in Table 3.

In all cases, the restore target was a location on the Windows client different from the source location.

Table 6. Single-stream restore from the HPE StoreOnce

Data set	Elapsed Time (mm:ss)
1	01:02
2	02:18
3	21:30
4	25:34
5	41:44

When using Veritas NetBackup to restore data from the HPE StoreOnce, the deduplicated data is rehydrated as it is read from the HPE StoreOnce to be written back to the client. Restores from the HPE Cloud Bank Storage store on Scality must also be rehydrated during the restore operation, because the catalyst copy operation used by NetBackup copies the deduplicated data from the HPE StoreOnce to the HPE Cloud Bank Storage store. Data is restored from HPE Cloud Bank Storage stores by reading the data from the HPE Cloud Bank Storage object store on Scality, passing it through the HPE StoreOnce for rehydration, and then restoring it to the client. Because of this unique behavior, restore performance in this scenario cannot be compared with restore performance of other applications that do not make use of the HPE StoreOnce OST plugin and Catalyst Copy functions of the HPE StoreOnce.

[7] NetBackup scheduled these two data sets in one duplication operation.
[8] NetBackup scheduled these two data sets in one duplication operation (same as previous entry).

Table 7 shows the average time to restore each data set, restoring from the HPE Cloud Bank Storage store. NetBackup performs restores from the primary backup, which in this case is the backup set on the regular HPE StoreOnce Catalyst store. In order to restore from the secondary copy on the HPE Cloud Bank Storage store (i.e., reading from the Scality RING S3 Connector), those secondary copy sets must be promoted to be the primary copy. The restore target was a location on the Windows client different from the source location.

Table 7. Single-stream restore from the HPE Cloud Bank Storage store using NetBackup

Data set	NetBackup activity monitor		HPE Cloud Bank Storage store data jobs		
	Elapsed Time (mm:ss)	Throughput (KB/s)	Data Read	Data Throughput	Read Duration (mm:ss)
1	00:39	92,654	2.2 GB	97.8 MB/s	00:22
2	01:39	84,463	7.1 GB	87.3 MB/s	01:21
3	17:02	88,835	86.3 GB	85.8 MB/s	16:45
4	21:26	75,202	97.7 GB	77.0 MB/s	21:09
5	12:33	219,454	165.4 GB	224.7 MB/s	12:16

Commvault: best practices and configuration guidance

Commvault enables backup and restore operations via services provided from cloud storage vendors. Commvault has certified Scality RING object storage as a cloud storage provider, using the Amazon S3 storage API type.

This paper addresses the following two general use cases for Commvault:

- Use case 1: Backing up directly to HPE Apollo 4000 storage servers and HPE Scalable Object Storage with Scality RING
- Use case 2: Backing up to an HPE StoreOnce NAS share with auxiliary copy to HPE Apollo 4000 storage servers and HPE Scalable Object Storage with Scality RING

For use case 1, restores were done from the backups on Scality RING object storage. For use case 2, Commvault does not support the OST plugin for the HPE StoreOnce Catalyst, so HPE StoreOnce NAS shares were used for all backup operations where HPE StoreOnce was the primary backup target. Restores were done from the primary backup on the HPE StoreOnce, and also from the auxiliary copy on Scality RING object storage. All restores were done to a location on the Windows client different from the original source location.

Test environment

A single-site, six-node cluster of HPE Apollo 4000 storage servers and HPE Scalable Object Storage with Scality RING with the Scality S3 Connector was installed and configured as on-premises cloud storage. A critical step in the configuration of the S3 Connector is recording the user access key and secret key. These keys are necessary when creating the Cloud Storage Library in Commvault. Also, make note of the IP address or fully qualified domain name used for accessing the Scality RING object storage, which will be required when creating the Cloud Storage Library in Commvault.

The Commvault software used during this testing was installed and configured on an HPE ProLiant server running Windows.

Best practices

This Reference Configuration provides guidance on configuring the Scality RING object storage for use with Commvault, as well as details on how to configure the elements of Commvault to use Scality RING object storage as the primary backup target (use case 1) and for use as the auxiliary copy target (use case 2). For example configuration scenarios, refer to the following:

- Appendix A: Cloudberry Explorer configuration details on page 19
- Appendix B: Commvault configuration details on page 20

For a brief discussion of backup and restore performance, refer to Overview of backup and restore performance on page 11.

IBM Spectrum Protect: best practices and configuration guidance

With IBM Spectrum Protect version 8.1.1, Scality RING version 6.4.3 and higher is supported as a Spectrum Protect Cloud-Container Storage Pool type. This allows high-speed S3-Compliant Spectrum Protect backup and archive data to be written to an on-premises HPE Apollo/Scality Software-Defined Cloud Object Storage solution.

IBM Spectrum Protect supports the following two general use cases:

- Use case 1: Using HPE Apollo 4000 storage servers and HPE Scalable Object Storage with Scality RING as the primary storage pool in Spectrum Protect
- Use case 2: Using an HPE StoreOnce NAS share as the primary storage pool in Spectrum Protect, with HPE Apollo 4000 storage servers and HPE Scalable Object Storage with Scality RING as the copy storage pool

Only use case 1 is addressed in this paper. For additional information regarding use case 2, and more information about configuring IBM Spectrum Protect and the HPE StoreOnce, refer to the following links on the HPE and IBM websites:

- https://community.hpe.com/t5/Around-the-Storage-Block/What-s-up-with-HPE-StoreOnce-and-IBM-Spectrum-Protect-besides-a/ba-p/6828500
- http://www-01.ibm.com/support/docview.wss?uid=swg21599235

Test environment

The HPE Apollo/Scality RING with S3 Connector should already be installed and configured as on-premises cloud storage. A single-site, six-node cluster of HPE Apollo 4000 storage servers was used in this testing. A critical step in the configuration of the S3 Connector is recording the user access key and secret key. These keys are necessary when creating the Cloud Storage Pool in Spectrum Protect. Also, make note of the IP address or fully qualified domain name used for accessing the Scality RING object storage, which will be required when creating the Cloud Storage Pool.

Best practices

This Reference Configuration provides guidance on configuring the Scality RING object storage for use with IBM Spectrum Protect, as well as details on how to configure the elements of Spectrum Protect to use Scality RING object storage as the primary backup target. For an example configuration scenario, refer to the following:

- Appendix A: Cloudberry Explorer configuration details on page 19
- Appendix C: IBM Spectrum Protect configuration details on page 30

For a brief discussion of backup and restore performance, refer to Overview of backup and restore performance on page 11.

Veritas NetBackup: best practices and configuration guidance

Veritas NetBackup Cloud Storage enables backup and restore operations via services provided from cloud storage vendors. NetBackup Cloud Storage supports the following API types:

- Amazon S3
- EMC Atmos
- Microsoft® Azure
- OpenStack Swift

Scality RING object storage is a NetBackup certified cloud storage vendor. NetBackup supports two Scality RING options under the Amazon S3 storage API type:

- **Scality RING – LAN (S3)** for Scality S3 On-Premises Object and Cloud storage, optimized for LAN
- **Scality RING – WAN (S3)** for Scality S3 Multi-Cloud storage, optimized for multi-site

The following two use cases are described in this paper:

- Use case 1: Scality RING as the direct target of NetBackup backup and restore operations.
- Use case 2: Scality RING configured as external object storage for an HPE Cloud Bank Storage store, which, along with an HPE StoreOnce Catalyst store, becomes a target for NetBackup backup/duplication (copy) operations.

Test environment

The Scality RING object storage solution is running on HPE Apollo 4000 servers acting as storage nodes. A single-site, six-node Apollo 4000/Scality RING was installed and the Scality S3 Connector was configured. A critical step in the configuration of the Scality RING S3 Connector is recording the user access and secret keys required when creating both the NetBackup Cloud Storage Server and the HPE Cloud Bank Storage store.

The NetBackup Master Server software was installed and configured on an HPE ProLiant server running Windows. The NetBackup Media Server software was installed and configured on two HPE ProLiant servers running Windows, with a third installation of Media Server on a virtual machine running Red Hat® Enterprise Linux®.

The HPE StoreOnce Catalyst NetBackup OST plugin was installed on the two Windows NetBackup Media servers. A Catalyst store was created on an HPE StoreOnce System. An OpenStorage Storage Server was configured on the NetBackup Master Server with the disk pool volume referencing the previously created Catalyst store.

Best practices

This Reference Configuration provides guidance on configuring the Scality RING object storage for use with Veritas NetBackup, as well as details on how to configure the elements of NetBackup to use Scality RING object storage as the primary backup target (use case 1) and for use as external object storage for an HPE Cloud Bank Storage store (use case 2).

For example configuration scenarios, refer to the following:

- Appendix A: Cloudberry Explorer configuration details on page 19
- Appendix D: Veritas NetBackup configuration details on page 32

For a brief discussion of backup and restore performance, refer to Overview of backup and restore performance on page 11.

Summary

IT is struggling to keep up with the demands of the business, which include a push for cloud services and capabilities, while at the same time minimizing costs. A majority of the IT budget is typically spent on maintaining existing systems, so IT has neither the budget nor the expertise to support a transformation to a hybrid-IT infrastructure. IT organizations need a solution that can meet the demands of all their workloads in a consistent manner with the flexibility to move workloads across the hybrid IT spectrum—private cloud, public cloud, and traditional IT—to adjust their *right mix* as business demands change.

Data is growing exponentially and 80% of newly created data is unstructured. To solve the problem of explosive growth of backup and archival data and ever-increasing costs, HPE Scalable Object Storage with Scality RING provides a solution that maximizes storage density and optimizes your cost of ownership. The HPE and Scality solution is easy to deploy, simple to grow, and built to create the right balance of protection, performance, and cost for your petabyte-scale storage needs.

The Scality RING is a simple-to-configure and simple-to-manage, software–based storage architecture. Because data protection is built-in, Scality software reduces the overall storage footprint, as compared to traditional object storage solutions that require data replication. Yet Scality RING object storage maintains the durability and availability that enterprise data assets require, providing a standards-based converged infrastructure solution that can help solve data scalability problems today. Combining industry-leading backup applications with HPE Scalable Object Storage with Scality RING and utilizing storage-density-optimized HPE Apollo 4000 storage server systems delivers the performance and protection of an on-premises backup solution with the flexibility and economics of the cloud.

Implementing a proof-of-concept

As a matter of best practice for all deployments, HPE recommends implementing a proof-of-concept using a test environment that matches as closely as possible the planned production environment. In this way, appropriate performance and scalability characterizations can be obtained. For help with a proof-of-concept, contact an HPE Services representative (hpe.com/us/en/services/consulting.html) or your HPE partner.

Appendix A: Cloudberry Explorer configuration details

There are several tools and applications that provide the ability to create and view buckets on Scality object storage. One such tool is CloudBerry Explorer, a free Amazon S3 browser that provides the ability to create and view the buckets to be managed by the backup applications. To use CloudBerry Explorer to create the buckets, perform the following:

1. Add an account specification to CloudBerry to access the Scality S3 Connector. Launch CloudBerry Explorer and select **File → New S3 Compatible Account**.
2. Select **Scality** as the cloud storage provider.
3. Enter a descriptive account name to display.
4. For **Service point**, enter the IP address or fully qualified domain name of the S3 Connector, as well as the service port (80).
5. Enter the **access key** and **secret key** that were generated when the S3 Connector and user account were configured on the Scality object storage.
6. Un-check the **Use SSL** box before completing the account definition, since SSL is not used with Scality object storage.
7. Click **Test Connection** to verify that the connection details and access keys are correct, and that the server can connect to the HPE Scalable Object Storage with Scality RING. If everything is correct, you see a popup window saying "Connection success".
8. Click **Close** on the **Connection success** window, and click **OK** to save the settings and create the new storage account in the CloudBerry user interface.

A completed **Add New Scality Storage Account** dialog box is shown in Figure 2.

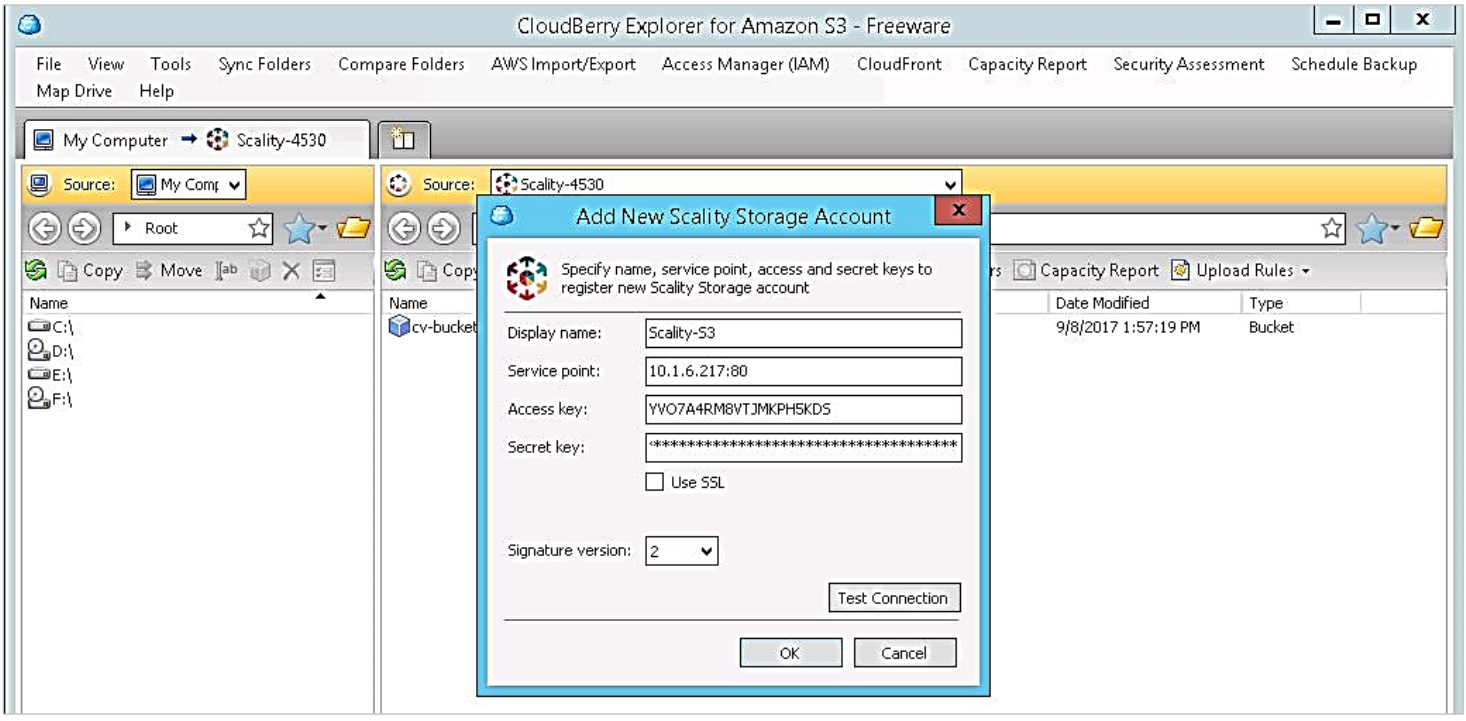

Figure 2. Using CloudBerry to create a new Scality storage account

To create a new bucket using CloudBerry Explorer, perform the following:

1. Select the storage account on Scality S3 as the **Source**.
2. Click the  icon (blue cube with a star), shown circled in Figure 3. This is the **New Bucket** icon.
3. Enter a descriptive name and click **OK**.
4. The newly created bucket appears in the CloudBerry Explorer display and is also be available for use in the backup application.

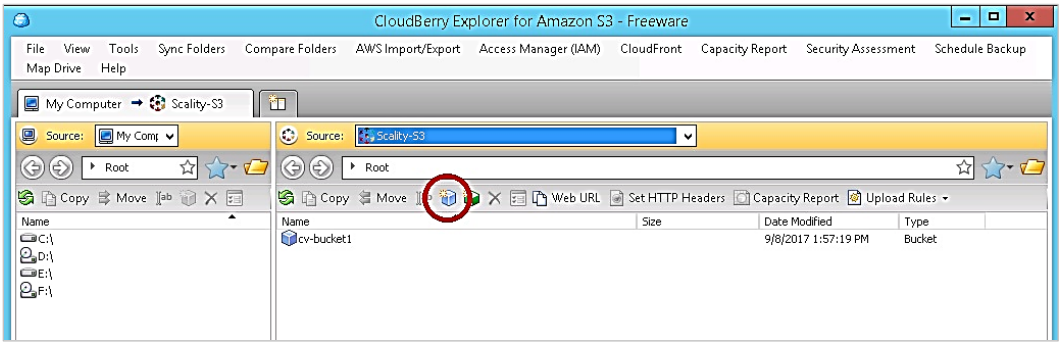

Figure 3. Using CloudBerry to create and view buckets in Scality RING

Caution

CloudBerry Explorer allows you complete control of the S3 buckets, as well as their contents. This includes adding and deleting buckets and files at will. Use CloudBerry only to create the buckets needed by the backup applications and the HPE StoreOnce, or to view buckets and contents. Be careful to not delete any buckets or files used by the backup applications or by the HPE Cloud Bank Storage store.

Appendix B: Commvault configuration details

This section describes how to configure a Scality RING – LAN (S3) Cloud Storage Server with Commvault software, including two example configuration use cases:

- Use case 1: Backing up directly to HPE Apollo 4000 storage servers and HPE Scalable Object Storage with Scality RING
- Use case 2: Backing up to an HPE StoreOnce NAS share with auxiliary copy to HPE Apollo 4000 storage servers and HPE Scalable Object

Creating buckets with CloudBerry Explorer

When using HPE Scalable Object Storage and the Scality S3 Connector with Commvault, you must specify a bucket name that already exists in Scality object storage. Commvault does not include a client interface for creating or viewing buckets on Scality; they must be created using a separate application.

Use an application, such as CloudBerry Explorer, to create the buckets for use with Commvault, as shown in Appendix A: Cloudberry Explorer configuration details on page 19.

Important: Implementing a proof-of-concept

The test scenarios performed for this document were intended to approximate a few common use cases for Enterprise Backup to HPE Scalable Object Storage with Scality RING deployments, where software-defined object storage adds value. *It is important to note that the step-by-step procedures documented may not match the steps necessary in your environment.* As a matter of best practice for all deployments, HPE recommends implementing a proof-of-concept using a test environment that matches the planned production environment as closely as possible. In this way, appropriate performance and scalability characterizations can be obtained. For help with a proof-of-concept, contact an HPE Services representative (hpe.com/us/en/services/consulting.html) or your HPE partner.

Use case 1: Backing up directly to Scality RING

Create the Cloud Storage Library

Log in to the Commvault CommCell administration console and create a library using Scality object storage, as shown in Figure 4 and Figure 5. This library serves as the primary backup target. To begin the process, right-click **Storage Resources → Libraries** in the left navigation tree and select **Add → Cloud Storage Library**, as shown in Figure 4.

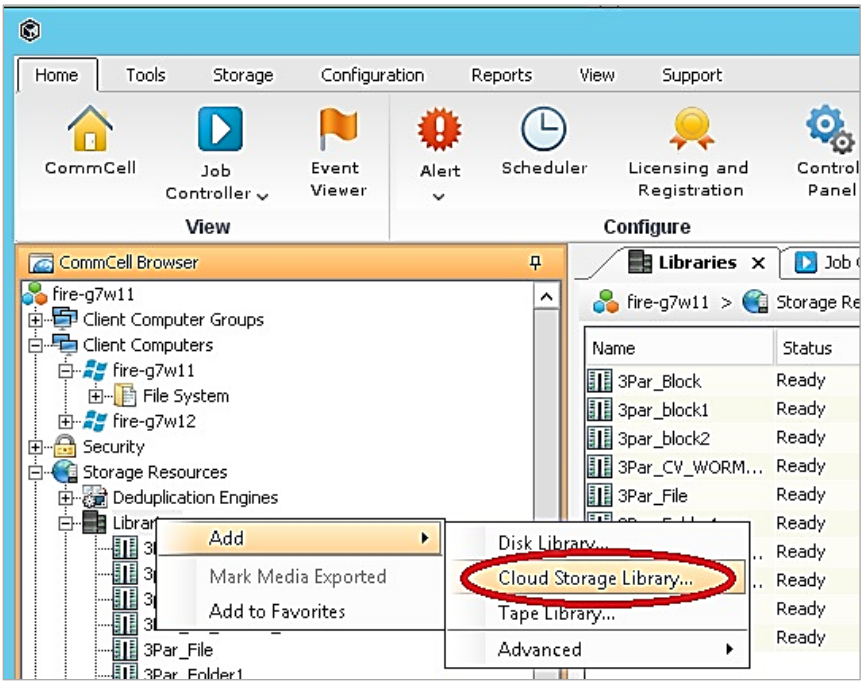

Figure 4. Create a new Cloud Storage Library

When the **Add Cloud Storage** dialog box opens, complete the fields as described below. A completed **Add Cloud Storage** dialog box is shown in Figure 5.

1. In the **Add Cloud Storage** dialog box, enter a descriptive name for the new library.
2. For **Type**, select **Amazon S3**. This specifies the correct API for use with Scality object storage.
3. Select the proper media agent. There may be only one listed, unless you have configured multiple media agents.
4. Under Access Information, set **Authentication** to **Access & Secret Keys**.
5. Set the **Service Host** to the IP address or fully qualified domain name of the host where the S3 Connector is configured.

Note
The default configuration for the S3 Connector uses HTTP. The Service Host entry must include the `http://` prefix and specify `port 80` at the end, as shown in Figure 5.

6. Copy and paste the **access key** and **secret key** values into the appropriate fields. These keys were created when the user account was created at the time the S3 Connector was installed and configured in the Scality RING.
7. Enter the **Bucket** name that was created previously. When configuring the Cloud Storage Library in Commvault, the bucket name must already exist.
8. Leave **Storage Class** set to the default value of **Standard**.
9. If a proxy server is needed in your configuration, click the **Advanced** tab to enter the appropriate details for proxy address, port, and access credentials.
10. Click **OK** to close the **Add Cloud Storage** dialog box and to create the cloud library.

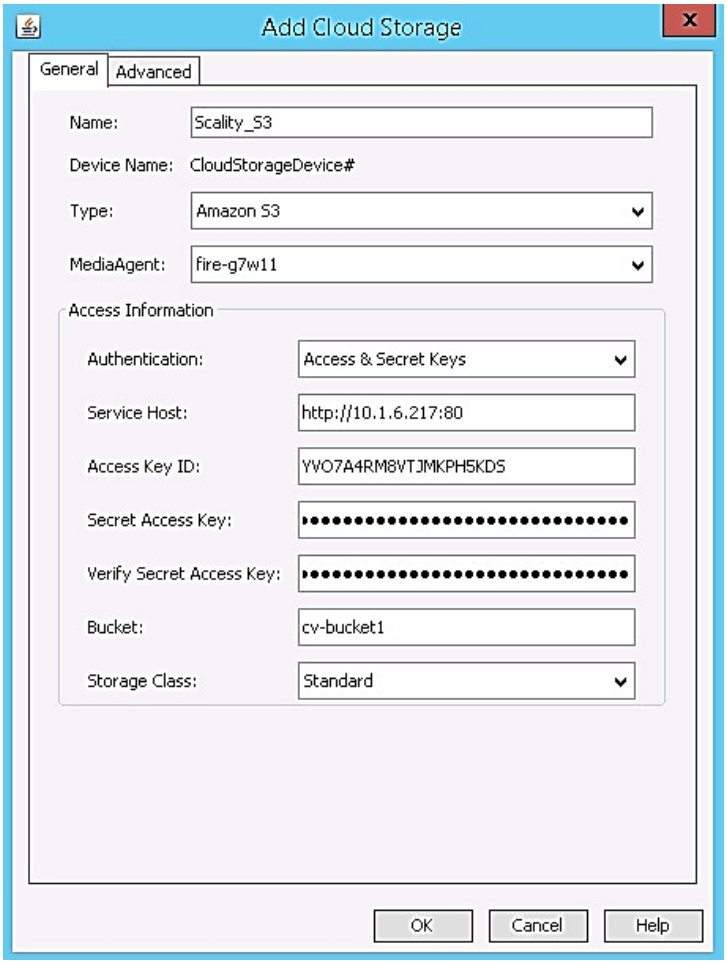

Figure 5. Creating a cloud storage library mapping to the Scality object storage

When the library has been created successfully, it will appear in the list of libraries configured in the CommCell browser with a status of **Ready** as shown in Figure 6.

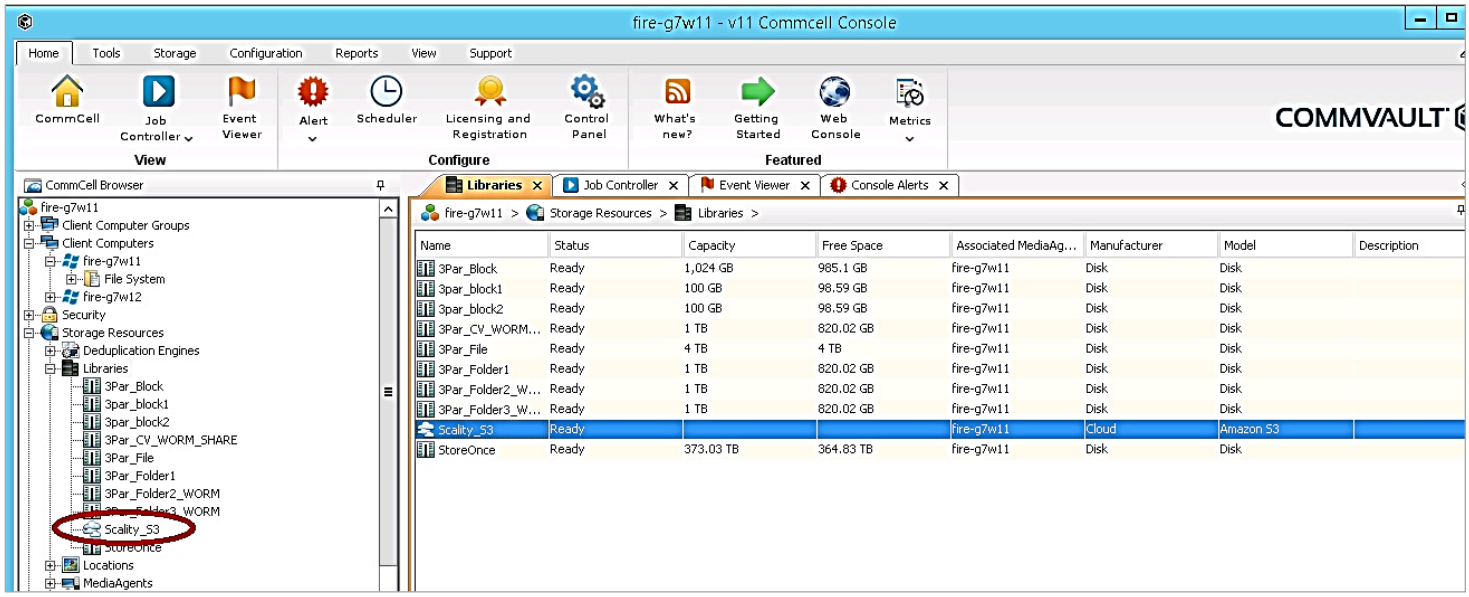

Figure 6. Displaying a successfully created Cloud Storage Library in the CommCell browser

Create the Storage Policy

After the cloud storage library has been successfully created, proceed with creation of the storage policy as you normally would for backups to a disk library in Commvault. When prompted by the **Create Storage Policy Wizard** to select the library for primary copy, be sure to specify the cloud-storage library that was just created on Scality object storage. Follow the steps below:

1. In the Commvault CommCell console, expand **Policies**.
2. Right-click **Storage Policies** and select **New Storage Policy**.
3. In the **Create Storage Policy Wizard** window, select **Data Protection and Archiving** and click **Next**.
4. Enter a descriptive name and click **Next**.
5. Set the **Library for Primary Copy** to be the cloud storage library created earlier and click **Next**.
6. Select the **MediaAgent** to be used and click **Next**.
7. Accept the defaults for number of device streams (or change as needed) and click **Next**.
8. Specify whether to enable **Software Encryption** and click **Next**.
9. Specify whether to enable **Deduplication** and click **Next**.

Note

If Deduplication is to be used, specify a location for the Deduplication Database. The location for the Deduplication Database must be in a subdirectory; it cannot be at the root level of the directory path specified.

---

10. Review the entries and click **Finish**.
11. Expand the new **Storage Policy** just created; right-click the Primary copy and select **Properties**.

12. On the **Retention** tab of the **Storage Policy Copy properties of Primary** window, set the retention period as required by corporate policy, internal governance, or regulatory compliance.
13. Click **OK** to close the properties window and save the storage policy.

Create the Backup Set

Create a Backup Set to specify the content to be backed up to the cloud storage library and to establish a suitable schedule.

Backing up to Scality

After creation of the Backup Set in Commvault, the backup job can be allowed to run on its normal schedule (if configured for a schedule), or can be initiated manually. The backup operation writes the content specified in the Backup Set to the cloud storage destination on HPE Scalable Object Storage with Scality RING, using the retention settings in the Storage Policy created above.

To initiate a backup manually, perform the following steps:

1. Expand **Client Computers** → [client] → **File System** → [backup set]; then right-click the subclient name and select **Backup**.
2. Choose **Full** or **Incremental** for the **Backup Type**, and determine whether to backup *immediately* or to *schedule* the backup. If Incremental is selected, the first backup will be automatically changed to a Full.
3. Click **OK** to save settings and queue the backup for immediate or scheduled execution, depending on your selection.
4. Monitor the status of the restore job on the Job Controller tab of the CommCell Console window.

Restore from backup on Scality

Content can be easily restored from the Scality RING using the normal **Browse and Restore** functions of the Commvault interface.

Use case 2: Backing up to an HPE StoreOnce NAS share with copy to Scality RING

Create the Disk Library for the primary backup location

Creating the library which maps to the HPE StoreOnce NAS share to be used as the primary backup location is similar to creating the cloud storage library using Scality RING object storage, described above, with some important differences.

1. Use the HPE StoreOnce user interface to create a NAS share on the HPE StoreOnce.
2. From the Commvault CommCell Console, right-click **Storage Resources** → **Libraries** in the left navigation tree and select **Add** → **Disk Library**.

3. Create a Disk Library that maps to the HPE StoreOnce NAS share, as shown in Figure 7.

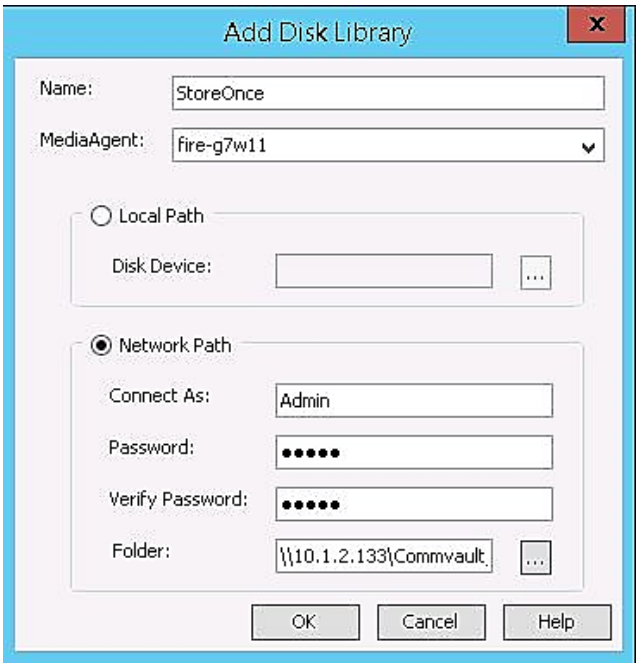

Figure 7. Creating a disk library mapping to an HPE StoreOnce NAS share

Create the Cloud Storage Library for the auxiliary copy location

1. In the Commvault CommCell Console, right-click **Libraries** in the left navigation tree and select **Add → Cloud Storage Library**, as shown previously in Figure 4.
2. In the **Add Cloud Storage** dialog box, enter a descriptive name for the new library.
3. For **Type**, select **Amazon S3**. This specifies the correct API for use with Scality object storage.
4. Select the proper media agent. There may be only one listed, unless you have configured multiple media agents.
5. Under Access Information, set **Authentication** to **Access & Secret Keys**.
6. Set the **Service Host** to the IP address or fully qualified domain name of the host where the S3 Connector is configured.

Note

The Service Host entry must include the `http://` prefix and specify `port 80` at the end, as shown in Figure 5.

---

7. Copy and paste the **access key** and **secret key** values into the appropriate fields. These keys were created when the user account was created at the time the S3 Connector was installed and configured in the Scality RING.
8. Enter the **Bucket** name that was created previously. When configuring the **Cloud Storage Library** in Commvault, the bucket name must already exist.
9. Leave **Storage Class** set to the default value of **Standard**.
10. If a proxy server is needed in your configuration, click the **Advanced** tab and enter the appropriate details for proxy address, port, and access credentials.
11. Click **OK** to close the **Add Cloud Storage** dialog box and create the cloud library.

Create the storage policy

Create a storage policy, as described earlier, and set the **Library** to be used as the disk library for the primary backup location on the HPE StoreOnce NAS share created above. Set the retention period according to company policy, internal governance, or regulatory guidance. The retention period for primary backups in this use case is normally relatively short (e.g., 30 days/4 cycles).

Create the copy policy

Create the auxiliary copy policy, which copies the contents of the primary backups to the Scality object storage for a longer retention time on more cost-efficient storage. Figure 8 shows the dialog box for specifying the settings for the copy policy.

1. In the Commvault CommCell Console, expand **Policies → Storage Policies** in the navigation tree on the left side of the window and select the storage policy just created.
2. Right-click the policy; then select **All Tasks → Create New Copy**.
3. Enter a descriptive name in the **Copy Name** field.
4. Under **Default Destination**, set the library to use the cloud storage library on Scality object storage, as shown in Figure 8.
5. Select the **MediaAgent** to use.
6. The retention period for auxiliary copies of backups in this use case is normally longer than the retention period for the primary copy. On the **Retention** tab, set the retention for a period longer than the retention of the primary backup, such as 365 days/52 cycles.
7. On the **Copy Policy** tab, select **All Backups** under Backup Selection, as shown in Figure 9. This causes all jobs where this policy is used to be copied to the auxiliary copy location on Scality.
8. Click **OK** to save the copy policy.

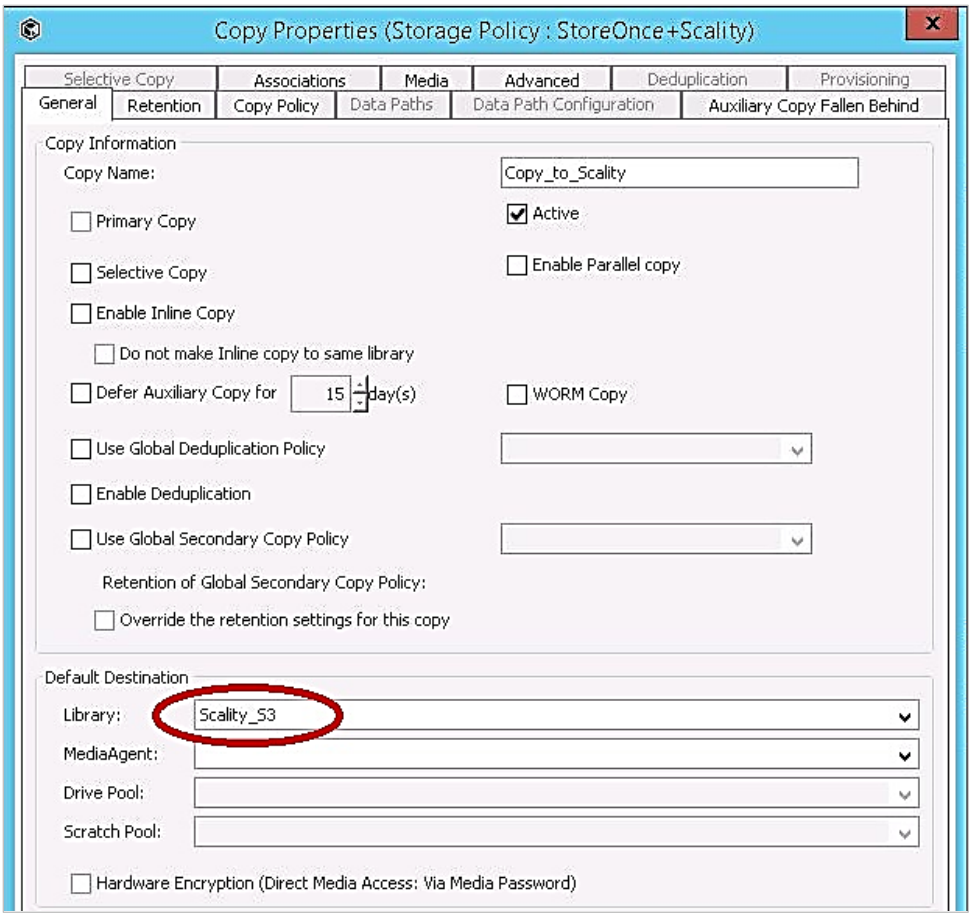

Figure 8. Creating an Auxiliary Copy Policy

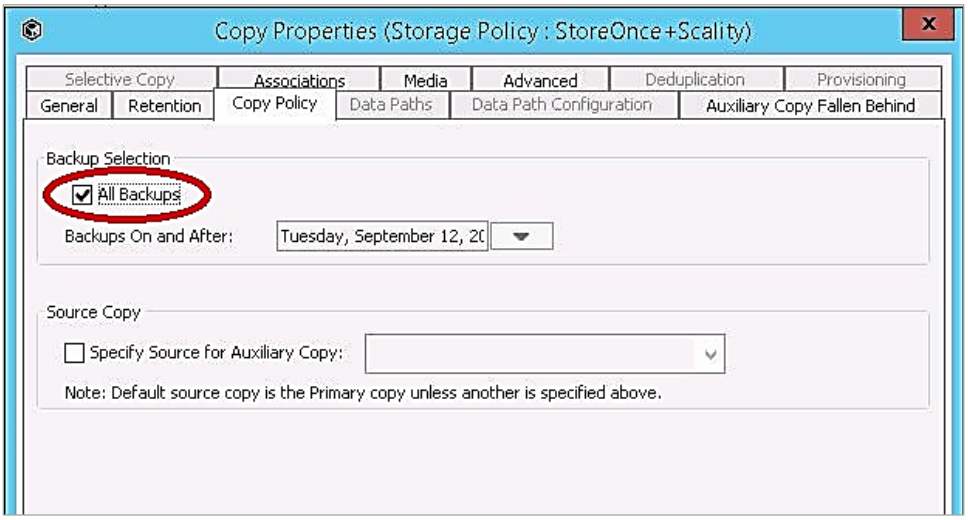

Figure 9. Creating an Auxiliary Copy Policy (continued)

Create the Backup Set

Create a Backup Set to specify the content to be backed up to the HPE StoreOnce and then copied to the cloud storage library. Establish a suitable schedule for the backups.

Backing up to the HPE StoreOnce

After creation of the Backup Set in Commvault, the backup job can be allowed to run on its normal schedule (if configured for a schedule), or can be initiated manually. The backup operation writes the content specified in the Backup Set to the NAS share on the HPE StoreOnce, using the retention settings in the Storage Policy created above. The auxiliary copy policy is not executed automatically after the backup job completes unless it is scheduled. The copy operation can be initiated manually, if desired, as described below.

Auxiliary copy to Scality

To run the Auxiliary Copy (secondary archive operation) manually, wait until the backup job is 100% complete. Then perform the following:

1. Right-click the policy and select **All Tasks → Run Auxiliary Copy**.
2. On the **General** tab of the **Auxiliary Copy Job Options** window, select the copy to run (there may be only one).
3. Accept the default values for other settings and click OK.
4. Status of the backup job can be monitored on the **Job Controller** tab of the CommCell Console window.

When the auxiliary copy operation executes, the Commvault media agent reads the primary backup from the HPE StoreOnce NAS share. If the data stream was deduplicated by the HPE StoreOnce as the primary backup was written, the data is rehydrated as it is read from the HPE StoreOnce. The media agent then writes the rehydrated data stream to the Scality object store via the S3 Connector.

Restore from primary backup on the HPE StoreOnce

Content can be easily restored from the Scality RING using the normal **Browse and Restore** functions of the Commvault interface. To be sure the data is restored from the primary copy on the HPE StoreOnce, set copy precedence to **1** as described below:

1. In the left navigation tree of the CommCell Console, expand **Client Computers →** [client] **→ File System →** [backup set]. Then right-click the subclient and select **Backup and Restore.**
2. On the **Time Range** tab, specify whether to restore files from the **Latest Backup**, or from a certain time or time range.
3. To verify that the content is restored from the primary backup copy, select the **Advanced Options** tab and either make sure the **Browse from copy precedence** box is not marked, as shown in Figure 10, or is marked and has the copy precedence set to **1**. The result will be the same whether the box is unmarked, or is marked and has the copy precedence set to **1**. Either method restores the data from the primary backup copy on the HPE StoreOnce.
4. Click the **View Content** button and choose the files to be restored from the primary copy.
5. Click **Recover All Selected** to restore the files.
6. In the **Restore Options for All Selected Items** dialog box, choose whether to overwrite files in the original location, the path the files should be restored to, and other options as necessary.
7. Click **OK** to initiate the restore.
8. Monitor the status of the restore job on the **Job Controller** tab of the CommCell Console window.

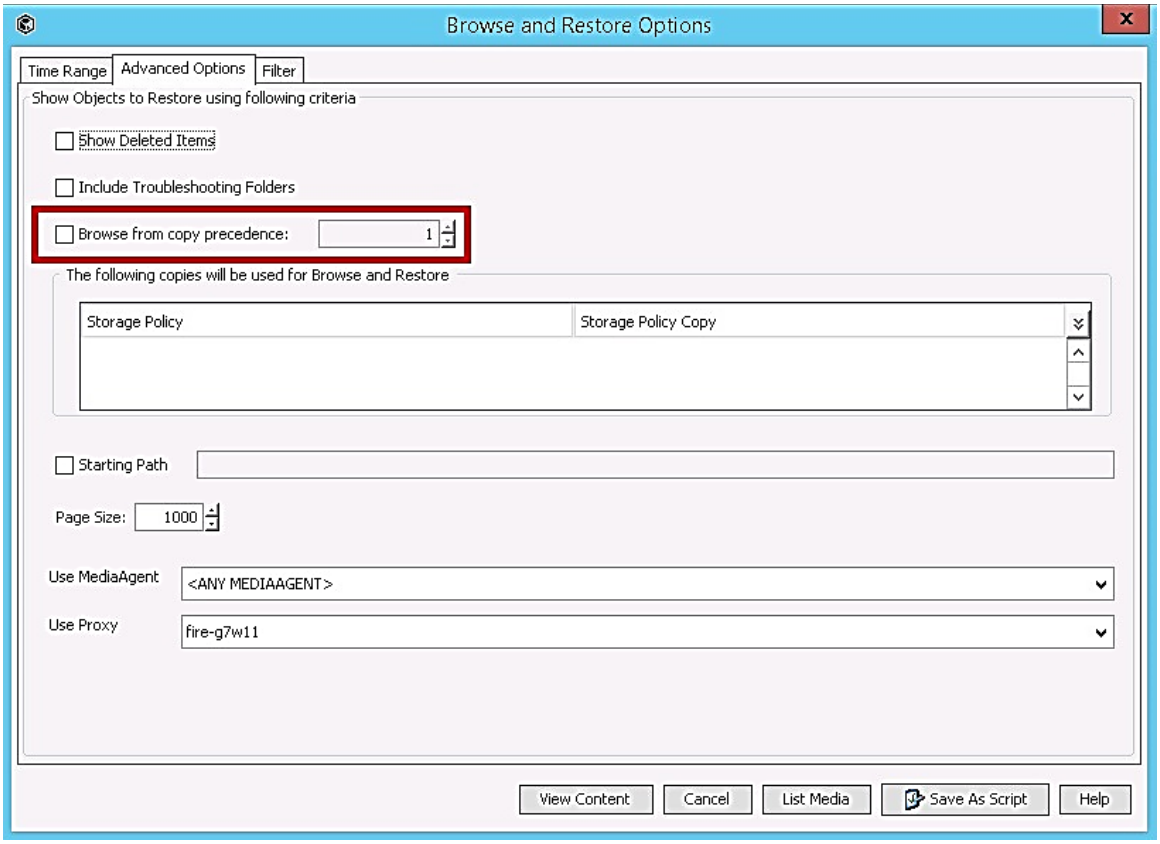

Figure 10. Restoring from primary backup on the HPE StoreOnce

Restore from auxiliary copy on Scality RING

Content from the auxiliary copy on the Scality RING can be restored easily using the normal **Browse and Restore** functions of the Commvault interface. The process is similar to restoring from the primary copy on the HPE StoreOnce, with one important difference, as shown in the steps below:

1. In the left navigation tree of the CommCell Console, expand **Client Computers** → [client] → **File System >** [backup set]. Then right-click the subclient and select **Backup and Restore**.
2. On the **Time Range** tab, specify whether to restore files from the **Latest Backup** or from a certain time or time range.
3. To verify that the content is restored from the auxiliary copy of the backup on Scality, select the Advanced Options tab.
4. Mark the box for **Browse from copy precedence** and set the copy precedence to **2** as shown in Figure 11. This ensures that the data will be restored from the auxiliary copy.
5. Click the **View Content** button and choose the files to be restored from the primary copy.
6. Click **Recover All Selected** to restore the files.
7. In the Restore Options for All Selected Items dialog box, choose whether to overwrite files in the original location, the path that the files should be restored to, and other options, as necessary.
8. Click **OK** to initiate the restore.
9. Monitor the status of the restore job on the Job Controller tab of the CommCell Console window.

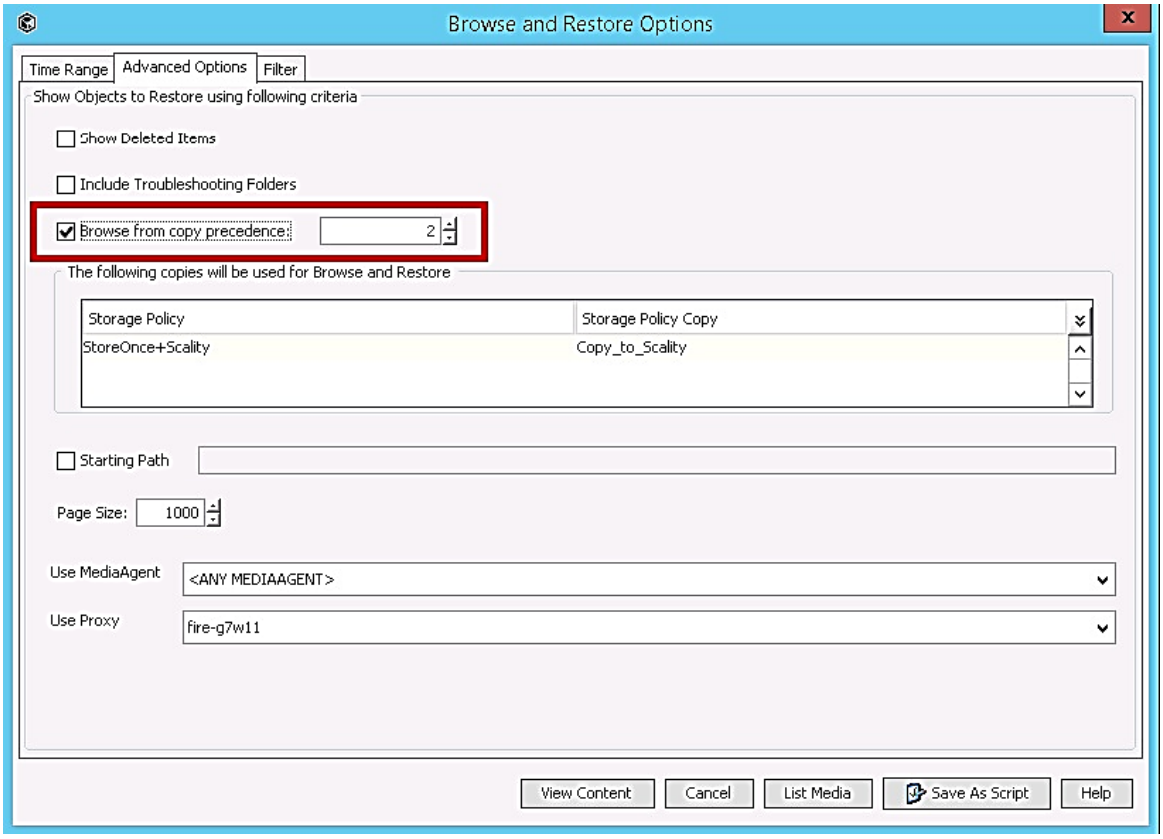

Figure 11. Restoring from the auxiliary backup copy on the Scality RING

Appendix C: IBM Spectrum Protect configuration details

This section describes how to configure a Scality RING – LAN (S3) Cloud Storage Server with IBM Spectrum Protect software, including an example configuration use case.

Creating buckets with CloudBerry Explorer

When using HPE Scalable Object Storage and the Scality S3 Connector with IBM Spectrum Protect, you must specify a bucket name that already exists in Scality object storage. IBM Spectrum Protect does not include a client interface for creating or viewing buckets on Scality; they must be created using a separate application.

Use an application, such as CloudBerry Explorer, to create the buckets for use with IBM Spectrum Protect, as shown in Appendix A: Cloudberry Explorer configuration details on page 19.

Important: Implementing a proof-of-concept

The test scenarios performed for this document were intended to approximate a few common use cases for Enterprise Backup to HPE Scalable Object Storage with Scality RING deployments, where software-defined object storage adds value. As a matter of best practice for all deployments, HPE recommends implementing a proof-of-concept using a test environment that matches the planned production environment as closely as possible. In this way, appropriate performance and scalability characterizations can be obtained. For help with a proof-of-concept, contact an HPE Services representative (hpe.com/us/en/services/consulting.html) or your HPE partner.

Example configuration use case

The steps below configure a Scality S3 Bucket on the Spectrum Protect Server. Due to the quantity of data protected by many Spectrum Protect environments, multiple S3 endpoints or a load balancer are strongly encouraged to optimize performance to the Scality S3 devices.

1. After creating the Spectrum Protect bucket on the Scality S3 Connector, use IBM Spectrum Protect to edit the bucket. Take care not to change the data in the bucket or edit the configuration settings for the bucket in any way.
2. Create a user account on the Scality S3 Connector using the access key ID and secret access key, so that IBM Spectrum Protect can access the S3 device.
3. Make sure this new user account has permission to store and delete data from the Spectrum Protect bucket.
4. Log in to IBM Spectrum Protect and define a **cloud-container storage pool** using the settings in Table 8, Table 9, and Table 10 below.

Table 8. Spectrum Protect required settings

Setting	Value
CLOUDTYPE	S3
IDENTITY	Secret access key
PASSWORD	Access key ID
CLOUDURL	http://cloud_object_storage_endpoint_IP_address https://cloud_object_storage_endpoint_IP_address

Table 9. Spectrum Protect optional settings

Setting	Value
CLOUDLOCATION	Default = offsite
MAXWRITERS	Default = NoLimit
ENCRYPT	Default = No
COMPRESS	Default = No for on-premises and Yes for off-site
ACCESS	Default = Readwrite
REUSEDELAY	Default = 1
DESCRIPTION	If spaces are used, enclose the description in quotes.

Table 10. Spectrum Protect best practice settings

Setting	Value
CLOUDLOCATION	ONPREMISE
MAXWRITERS	Either of the following: • As many streams as necessary to saturate the Spectrum Protect Server NIC links • NoLimit if the HPE Apollo/Scality RING is only hosting Spectrum Protect operations
ENCRYPT	No
COMPRESS	No
REUSEDELAY	>DRMDBBACKUPEXPIREDAYS

5. To configure the HPE Apollo/Scality S3 Cloud-Container Storage Pool for IBM Spectrum Protect, enter a command similar to the following:

```
define stgpool hpescalitys3-stgp stgtype=cloud \
   cloudtype=s3 cloudurl=http://scality-s3.hpe.com:8000 \
   identity=N7LNZMYB496GBUIQN97P password=ZRfIAMa3UqnAjZepXAdGMUGHwQrOFLrtGfwuYlcJ \
   bucketname=spbucket1 cloudlocation=onpremise maxwriters=50
```

In the CLI command above, CLOUDURL is the endpoint of the HPE Apollo/Scality S3 Connector. This value can be either a DNS entry or an IP address. The protocol (such as `https://` or `http://`) must precede the DNS or IP address at the beginning of the URL stanza. For optimal performance, CLOUDURL should be directed to an external load balancer. Additionally, multiple HPE Apollo/Scality S3 Connector endpoints can also be used. These addresses must be separated by a vertical bar (|) with no spaces, as in the following: `http://192.168.1.2|http://192.168.1.3|http://192.168.1.4|http://192.168.1.5`. Since the maximum length of the web address is 870 characters, an IP address may need to be used instead of a DNS entry.

Important
The CLOUDURL parameter is not validated by IBM Spectrum Protect until the first backup commences.

The `REUSEDELAY` parameter on the Storage Pool for the HPE Apollo/Scality S3 buckets should be set to a duration that exceeds the Spectrum Protect database backup retention period. `REUSEDELAY` specifies the number of days that must elapse in Spectrum Protect before deduplicated extents are deleted from the cloud storage pool. By setting this parameter to a value greater than the number of days specified in the `SET DRMDBBACKUPEXPIREDAYS` command, you make sure of your ability to restore the database to an earlier level since the references to files in the cloud storage pool are still intact and valid.

Performance considerations

An IBM Spectrum Protect best practice is to avoid storing certain client data types in cloud-container storage pools, such as Data Protection for VMware® control files and Data Protection for (legacy backups) SQL metadata files. The performance of a cloud-container storage pool relies on the network connection between the Spectrum Protect Server and the HPE Apollo/Scality S3 Connectors. If the RING is hosting more than Spectrum Protect Server operations and the LAN is oversubscribed, Spectrum Protect Backups and Archive performance could be impacted. Likewise, S3 delete operations are a multipart process. Deleting a large number of objects, or filespaces, or very large files from Spectrum Protect cloud-container storage pools can take considerable time. Depending on the Spectrum Protect Server architecture and the data type, single-stream performance can vary, ranging from approximately 150 to 250 MB/s for mixed-block I/O. Under these circumstances, a Spectrum Protect Server has the ability to saturate a single 10 GbE link with as few of 4-8 concurrent streams.

Contact your HPE Sales Representative for specific IBM Spectrum Protect documentation, which includes installation, configuration, and best practices for optimizing solution performance between IBM Spectrum Protect and HPE Storage appliances.

Appendix D: Veritas NetBackup configuration details

This section describes how to configure a Scality RING – LAN (S3) Cloud Storage Server with Veritas NetBackup software, including two example configuration use cases:

- Use case 1: Scality RING as the direct target of NetBackup backup and restore operations.
- Use case 2: Scality RING configured as external object storage for an HPE Cloud Bank Storage store, which, along with an HPE StoreOnce Catalyst store, become a target for NetBackup backup/duplication (copy) operations.

Creating buckets with CloudBerry Explorer

When using HPE Scalable Object Storage and the Scality S3 Connector with Veritas NetBackup, you must specify a bucket name that already exists in Scality object storage.

Use an application, such as CloudBerry Explorer, to create the buckets for use with Veritas NetBackup, as shown in Appendix A: Cloudberry Explorer configuration details on page 19.

Important: Implementing a proof-of-concept

The test scenarios performed for this document were intended to approximate a few common use cases for Enterprise Backup to HPE Scalable Object Storage with Scality RING deployments where software-defined object storage adds value. As a matter of best practice for all deployments, HPE recommends implementing a proof-of-concept using a test environment that matches the planned production environment as closely as possible. In this way, appropriate performance and scalability characterizations can be obtained. For help with a proof-of-concept, contact an HPE Services representative (hpe.com/us/en/services/consulting.html) or your HPE partner.

Viewing buckets with CloudBerry Explorer

NetBackup and HPE StoreOnce do not provide a client interface for viewing the Scality S3 Connector account buckets and files. Use a tool, such as CloudBerry Explorer, to view the buckets and files that NetBackup creates and manages. Figure 12 shows a list of buckets in use by NetBackup storage servers.

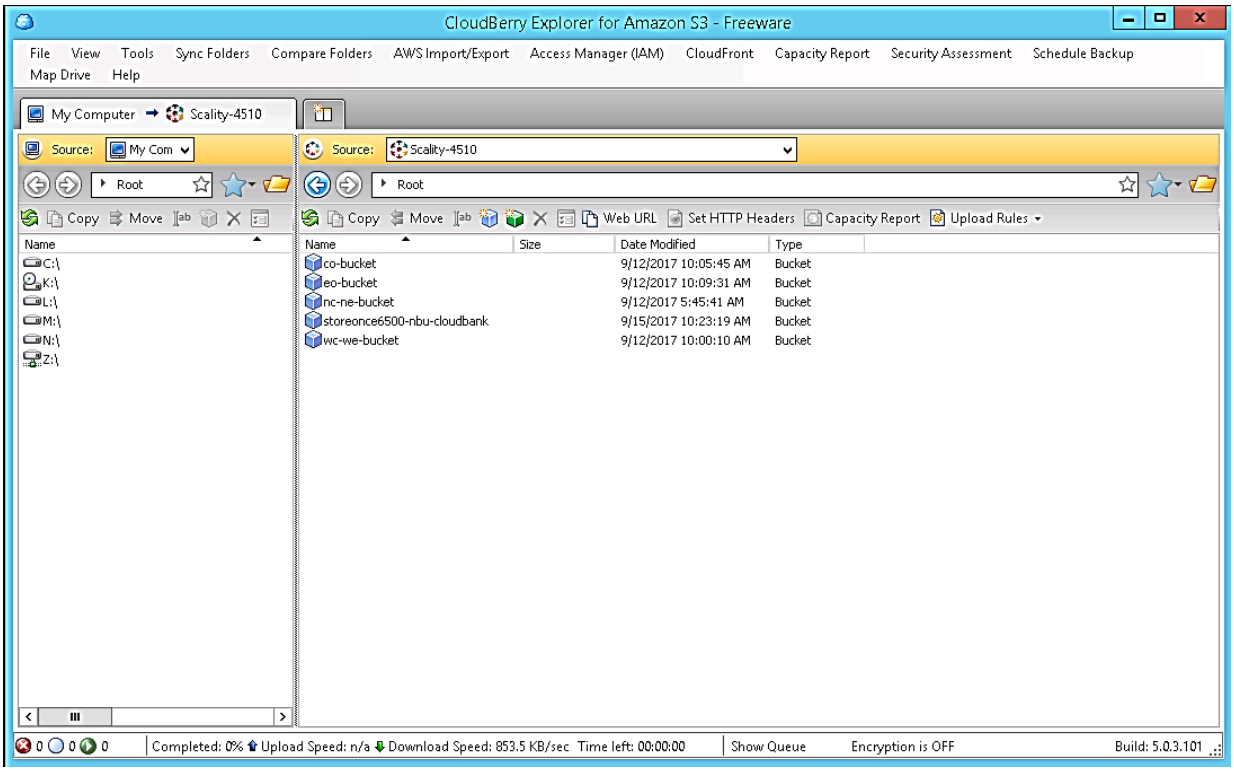

Figure 12. Using CloudBerry Explorer to see the buckets in use by NetBackup

Use case 1: Backing up directly to Scality RING

Configuring a NetBackup Cloud Storage Server

NetBackup incorporates a Cloud Storage Server configuration wizard to facilitate the cloud storage setup and storage provisioning. Cloud storage provisioning happens entirely through the NetBackup interface.

Log in to the NetBackup Administration Console on the Master Server. The Details pane displays the available configuration wizards. Figure 13 shows the Details pane with the Cloud Storage Server configuration wizard highlighted.

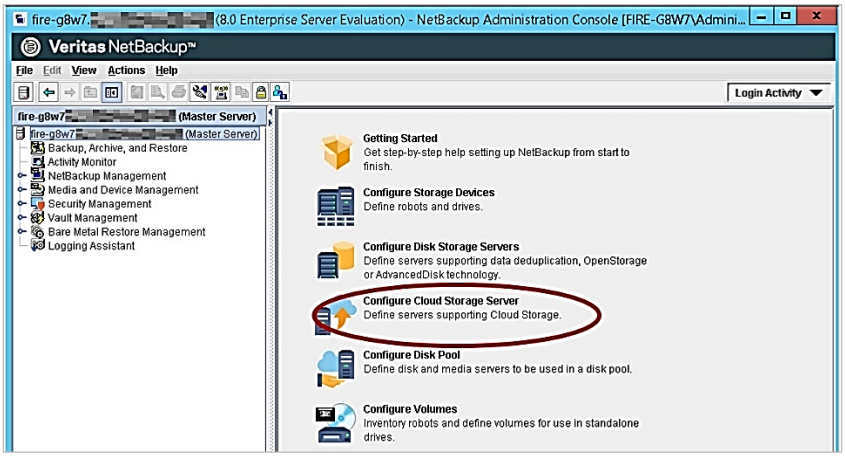

Figure 13. Choosing the Cloud Storage Server configuration wizard

Double-click **Configure Cloud Storage Server** to start the wizard, which begins with a welcome screen. After reviewing the information on the welcome screen, select **Next** to bring up the vendor-selection screen. The default for this screen is to display a list of all the cloud storage providers for all storage API types supported by NetBackup. The **Storage API type** field offers a pull-down menu with many options. To focus only on Amazon S3 providers, select **Amazon S3** from the list of API types. This narrows down the list of cloud storage providers to those vendors supporting this Amazon API type. Enter **Scality** in the search field to display only the two Scality RING options. Figure 14 shows the selection of the Amazon S3 storage API type and the results of a search for providers containing the string "Scality".

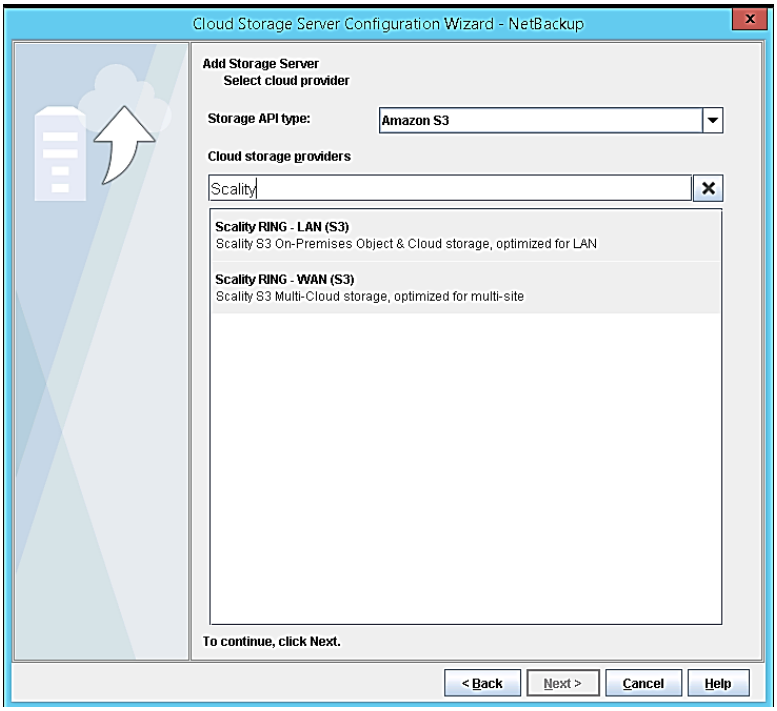

Figure 14. Displaying Scality RING as an Amazon S3 API cloud storage provider

Highlight the provider **Scality RING – LAN (S3)** and click **Next**. This brings up the Add Storage Server panel, shown in Figure 15. The Service host and Storage server name fields are blank.

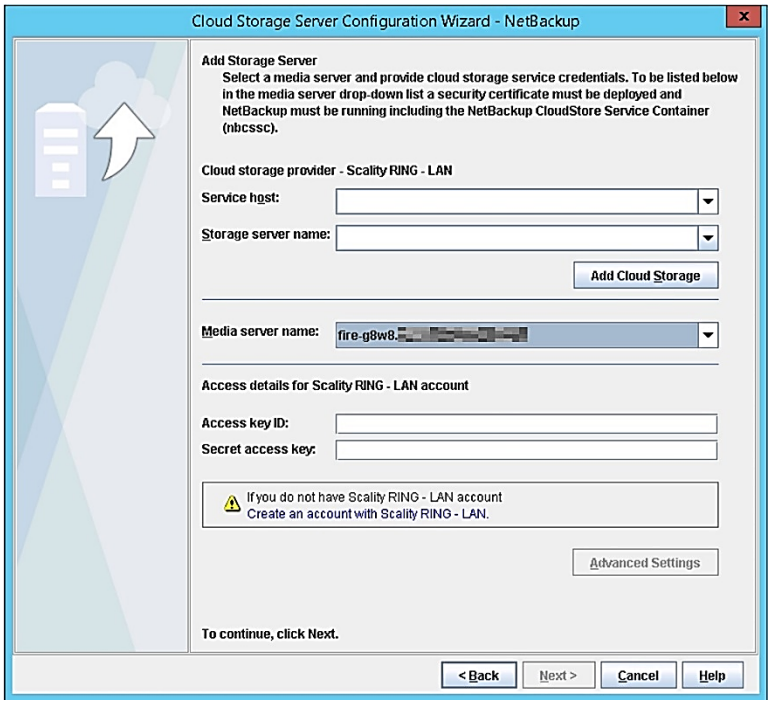

Figure 15. Adding a cloud storage server

To add a new cloud storage server, click the **Add Cloud Storage** button. This brings up the Add Cloud Storage panel, shown in Figure 16. In the Service host field, enter the IP address of the Scality RING storage node, which hosts the S3 Connector. The Storage server name field is automatically populated based on the IP address. Figure 16 shows the completed entries.

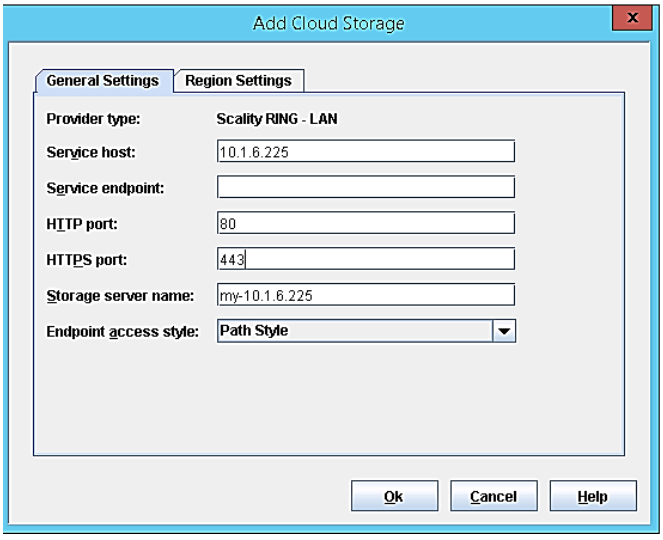

Figure 16. Specifying the Service host entry and resulting Storage server name

Click **OK** to return to the Add Storage Server panel. You now see the **Service host** and **Storage server name** fields completed. Use the pull-down option in the **Media server name** field to choose the initial media server to associate with this cloud storage server. When the S3 Connector was installed in the Scality RING, a user account was created, which was given an access key and a secret access key. Copy and paste those values in the appropriate account access fields. Figure 17 shows a completed Add Storage Server screen.

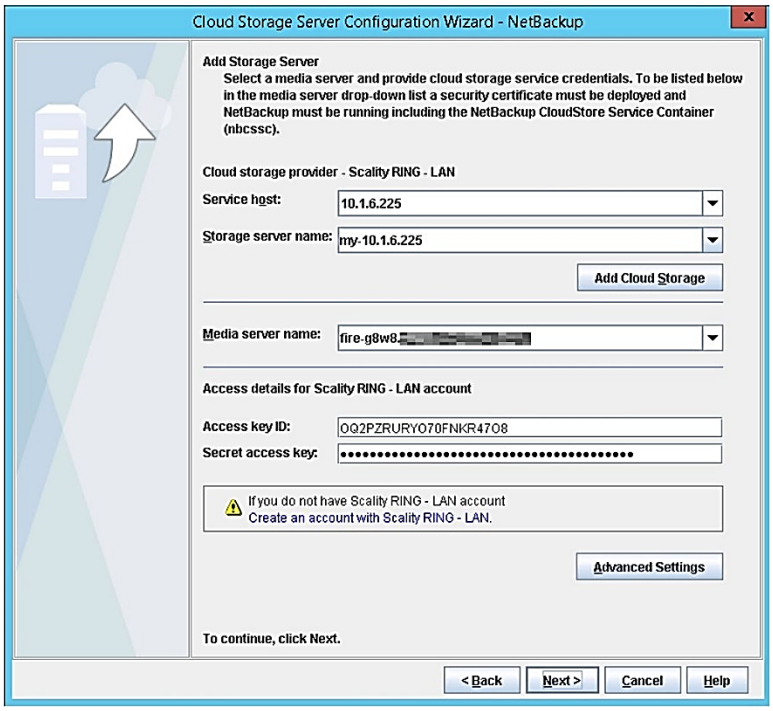

Figure 17. Completed Add Storage Server screen

Important

Before proceeding with the wizard, you must click **Advance Settings** and deselect the **Use SSL** button. This button is selected by default and must be changed. The Scality S3 Connector does not use SSL communications.

Click **Next** to proceed to the next step in the wizard. Figure 18 shows a panel that asks you to select compression and encryption options for this storage server. You can choose neither, both, or only one of the settings.

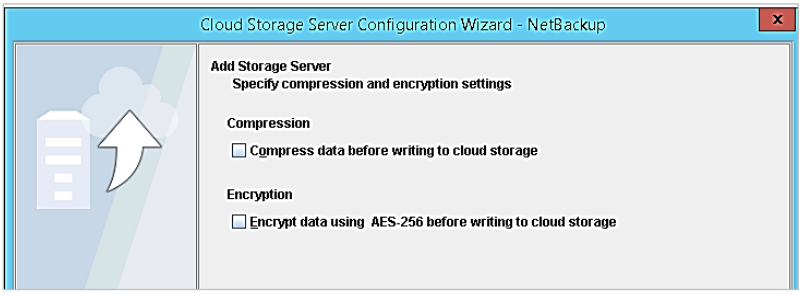

Figure 18. Choosing compression and encryption options for the new storage server

The choice of compression and encryption options cannot be modified after the storage server is created. Before you can move on with the wizard, a pop-up appears asking you to confirm your compression and encryption choices, as shown in Figure 19.

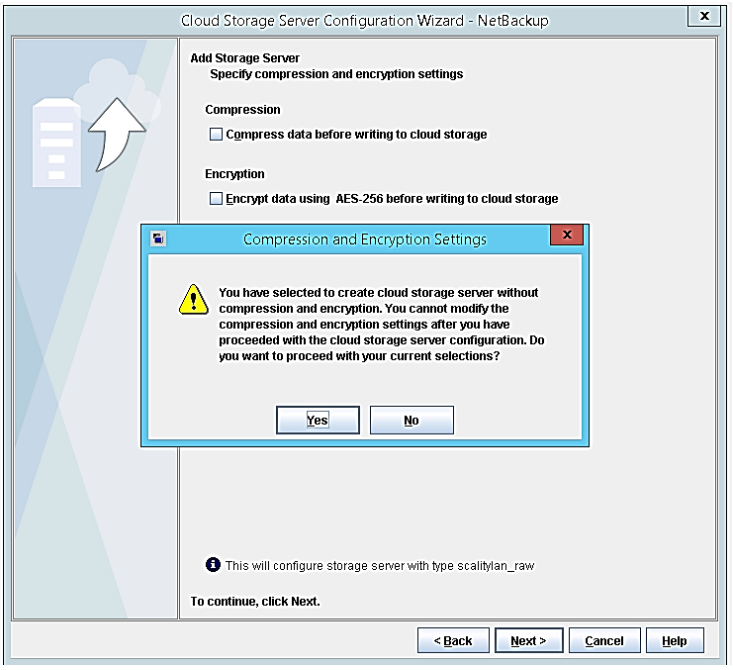

Figure 19. Compression and encryption option settings that cannot be modified later

After clicking **Yes** to verify the compression and encryption settings, click **Next** to bring up another verification screen. Use the **Back** button if you wish to make modifications to the settings for this storage server. Figure 20 shows the verification screen with the **Storage server type** designation highlighted. For this storage server, the Storage server type is **scalitylan_raw**. Note that this designation also appears in the information statement at the bottom of the compression and encryption screen (Figure 19).

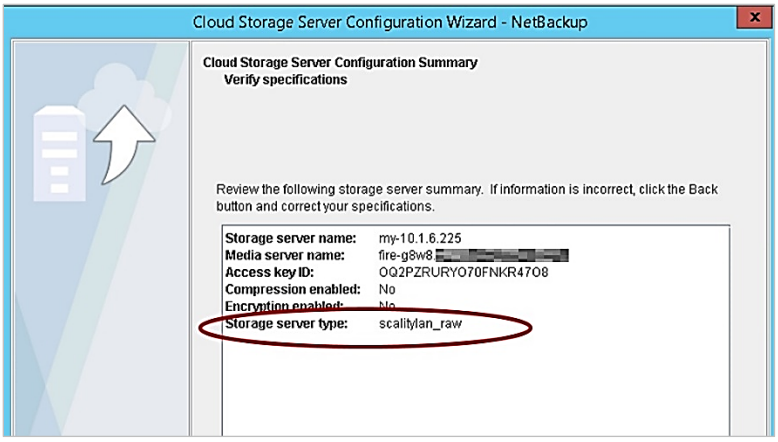

Figure 20. Storage Server configuration summary

Note

The Storage server type entry shown in Figure 20 is listed as `scalitylan_raw` because this storage server was created without compression or encryption. If compression only is selected when configuring a storage server, the storage server type will be `scalitylan_rawc`. If encryption only is selected for the storage server, the storage server type will be `scalitylan_crypt`. If both compression and encryption are selected for the storage server, the storage server type will be `scalitylan_cryptc`. (See Figure 25.)

Click **Next** to accept the configuration and complete creating the storage server. One key step in this process is to see a check mark next to the **Adding credentials** task. This confirms that the NetBackup media server can access and communicate with the Scality S3 Connector with the configuration and access information that has been provided.

After the successful creation of the cloud storage server, you have the option to close the wizard at this point, which will require you to manually create the disk pool and storage unit, or click **Next** to continue with the wizard.

The next step is to configure the Disk Pool. Since this is a new pool, no volumes are associated with the pool, so you must click **Add New Volume**. The S3 API stores objects in containers called *buckets*. For the Scality S3 Connector, selecting **Add New Volume in the Disk Pool** causes the configuration wizard to bring up the **Create Buckets** panel, as shown in Figure 21. Enter the **bucket name** in the Bucket name field. Note that any letters in the bucket name must be all lowercase. NetBackup creates the bucket as part of this operation; the bucket does not have to exist already. The name chosen for the bucket, **nc-ne-bucket**, shown in Figure 21, reflects the fact that this cloud storage server is not configured for compression or encryption.

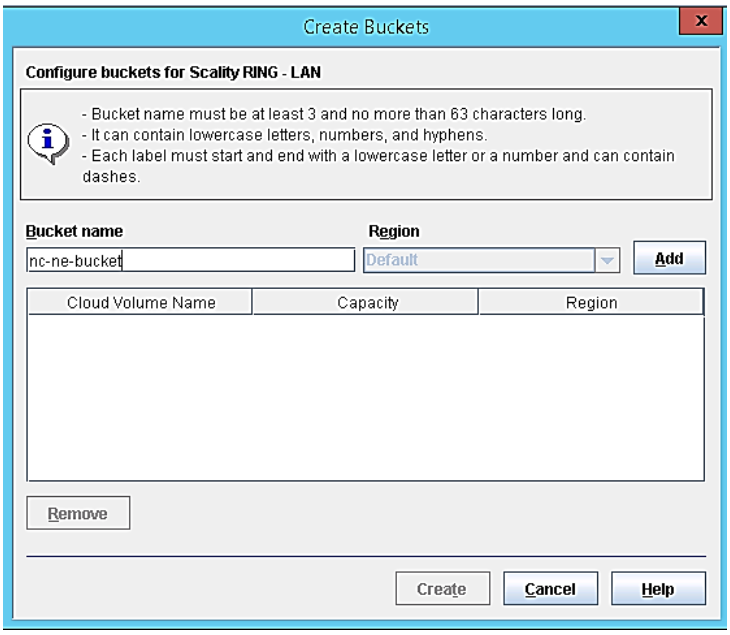

Figure 21. Specifying the bucket name

Click **Add** to add the bucket entry into the **Cloud Volume Name** panel (Figure 22).

Note

You cannot add another bucket. Each cloud storage server supports only one bucket. To use multiple buckets, you need to create multiple cloud storage servers.

Select the cloud volume name and click **Create** to complete creating the bucket for this disk pool.

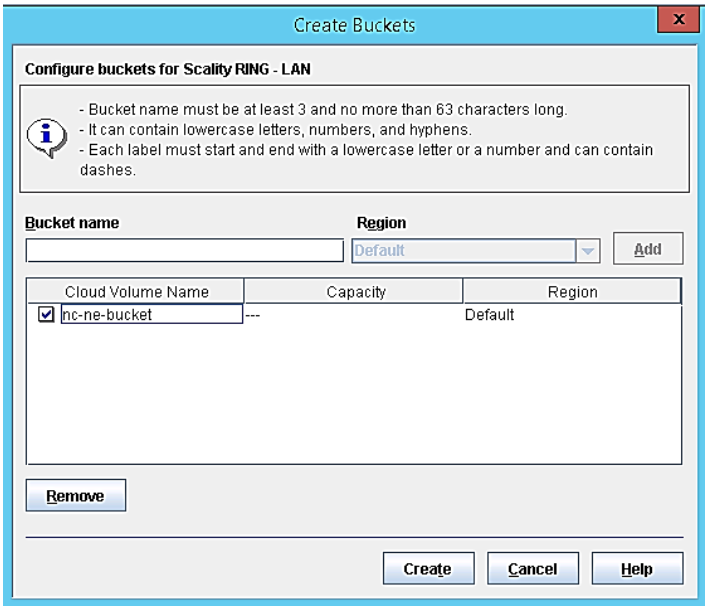

Figure 22. Selecting the cloud volume to associate with the disk pool

The next step is to provide a name for the Disk Pool (Figure 23). Optionally, you may add any comments to describe the disk pool.

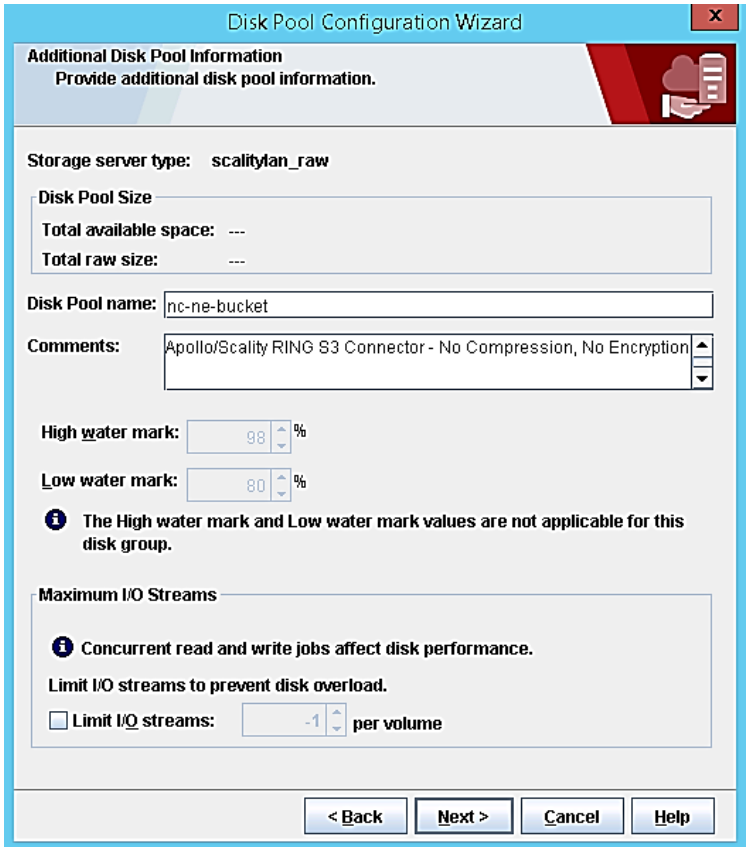

Figure 23. Assigning a name to the disk pool

Click **Next** to bring up the summary and confirmation screen. Review the entries, choosing **Back** if you wish to make modifications. If the Disk Pool summary information is correct, select **Next** to complete the Disk Pool Configuration Wizard. A disk pool configuration status screen appears. You have the option to close the wizard at this point, which requires you to manually create a storage unit, or click **Next** to continue with the wizard.

The next step is to create the storage unit to be associated with this disk pool. The Storage Unit Creation panel is shown in Figure 24. The Storage unit name field is filled in automatically with the name of the disk pool followed by `-stu`. You may choose to edit this field.

The Media Server selection defaults to use any available media server or you can optionally select only specific media servers. The choice of available media servers reflects the entry made at the start of the Add Storage Server wizard (Figure 15). Additional media servers can be added later by changing the properties of the storage server.

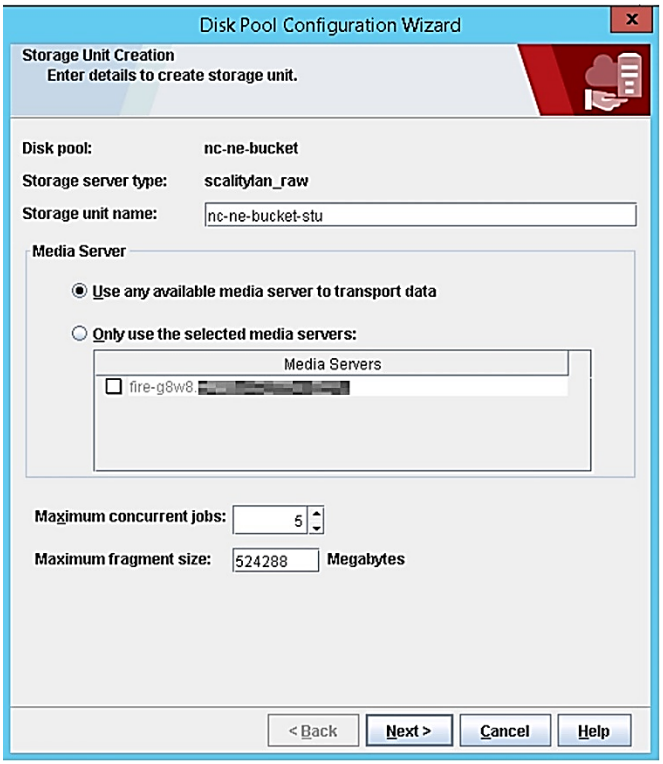

Figure 24. Creating a storage unit for the disk pool

Click **Next** to complete creating the storage unit. The final panel appears indicating that the disk pool configuration wizard is complete. Clicking **Finish** returns you to the NetBackup Administrator Console Detail panel.

Master Server properties – Cloud Storage

To review the cloud-storage hosts and their associated cloud storage servers, from the navigation tree of the NetBackup Administration Console, select **NetBackup Management → Host Properties → Master Servers**. Double-click the highlighted entry to bring up the Master Server Properties Panel. Figure 25 shows how to select **Cloud Storage** from the options in the navigation panel with the cloud storage service host 10.1.6.225 highlighted.

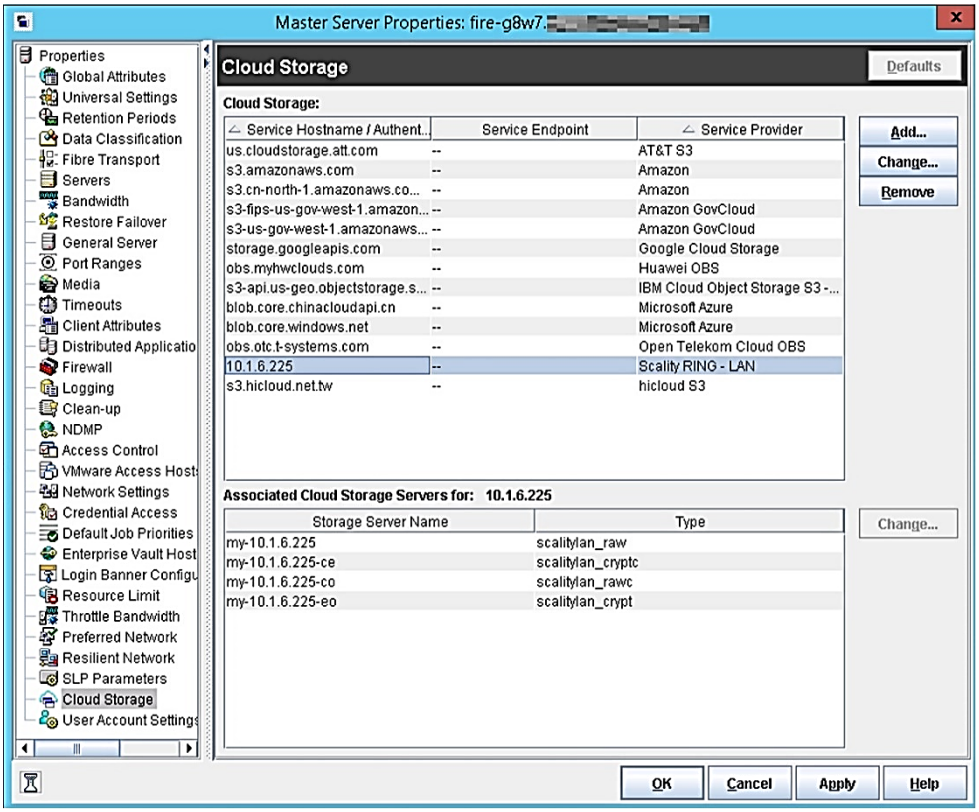

Figure 25. Displaying the cloud storage servers associated with the cloud-service host 10.1.6.225

Creating additional storage servers for a cloud-storage host

Figure 25 shows a total of four storage servers associated with one cloud-storage host. Veritas recommends that if you must enable a mix of compression and encryption in your cloud storage, you should assign a separate bucket for each combination. Since only one bucket can be assigned to a given storage server, using multiple buckets for compression and encryption requires creating additional storage servers.

To create these additional storage servers, you once again use the Cloud Storage Server Configuration Wizard (Figure 13). The Service host name in the **Add Storage Server** panel is populated with the service host name, as shown in Figure 25. You only need to enter the name of the new storage server you want to create in the **Storage server name** field. Figure 26 shows adding a storage server named `my-10.1.6.225-co` using the theme that this storage server will be configured to support compression only.

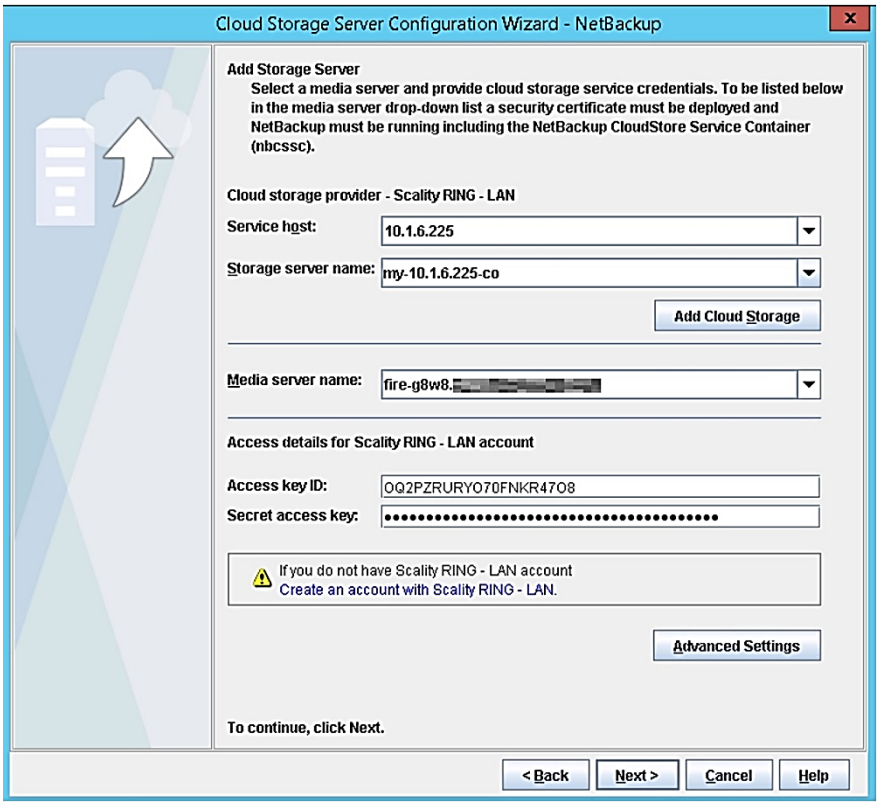

Figure 26. Adding a new storage server to an existing service host

Continue with the wizard and choose the encryption and compression option. (Figure 26 above shows an example with compression only.) Complete the wizard by creating a new disk pool (bucket) and storage unit associated with this storage server.

Specifying cloud storage units in a NetBackup Policy

A NetBackup Policy specifies the attributes, schedule, client server, and backup selection components of a backup operation. To write backups directly to the Scality RING S3 Connector, create a NetBackup policy as you normally would. The only necessary modification is to specify the cloud-server storage unit in the Policy storage definition field. Figure 27 shows the Attributes tab of the Change Policy screen with the pull-down menu expanded under the **Policy storage** field. The pull-down menu lists the possible storage units that may be selected. In Figure 27, the storage unit, `nc-ne-bucket-stu` is highlighted. Using this policy, non-compressed, non-encrypted backups will now be directed to the Scality S3 Connector.

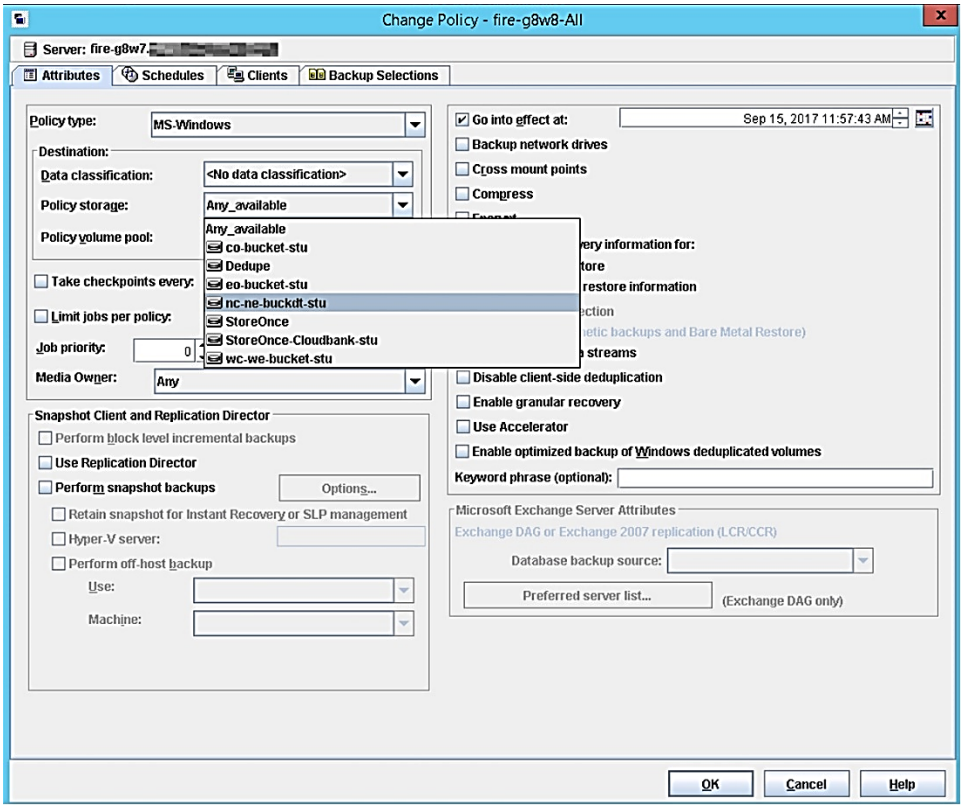

Figure 27. Selecting the Policy storage specification as part of the policy attributes

The policy is now complete and can be used in scheduled or manual backup operations.

Use case 2: Copy operations directed to HPE Cloud Bank Storage on Scality RING

HPE Cloud Bank Storage is an HPE StoreOnce feature that enables HPE StoreOnce to leverage external object storage for the long-term retention of copies of backup data sets. An HPE StoreOnce Catalyst Copy operation efficiently copies the backup data sets from an HPE StoreOnce Catalyst store to an HPE Cloud Bank Storage store. Directing HPE StoreOnce Catalyst copy operations is accomplished in NetBackup through a Storage Lifecycle Policy and the HPE StoreOnce Catalyst NetBackup OST plugin. Backups are first written to an HPE StoreOnce Catalyst Store. Then the NetBackup duplication (copy) operation invokes the Catalyst Copy feature to send a copy of the backup to an HPE Cloud Bank Storage store (writing data to the HPE Apollo/Scality RING using the Scality S3 Connector).

The following sections provide the steps necessary to incorporate an HPE Cloud Bank Storage store in NetBackup copy operations:

- Configuring an HPE Cloud Bank Storage Catalyst store using the Scality RING S3 Connector
- Creating a NetBackup storage server which uses the Cloud Bank Storage Catalyst store
- Creating a NetBackup Lifecycle Policy directing backups to an HPE StoreOnce Catalyst Store and duplication operations to a Cloud Bank Storage store
- Creating a NetBackup Policy which specifies the Storage Lifecycle Policy as the Policy storage

Configuring an HPE Cloud Bank Storage Catalyst store

From the HPE StoreOnce Management Console GUI, select **StoreOnce → StoreOnce Catalyst-Stores**. From the Stores display, select **Create** in the upper-right corner. Select the **Service Set** to which this store will belong and click **OK**. This will present you with the **New Store** screen, as shown in Figure 28. Notice that this screen is identical to the screen used to create a regular Catalyst Store with one exception—that being the last line of the panel—the option to choose HPE Cloud Bank Storage.

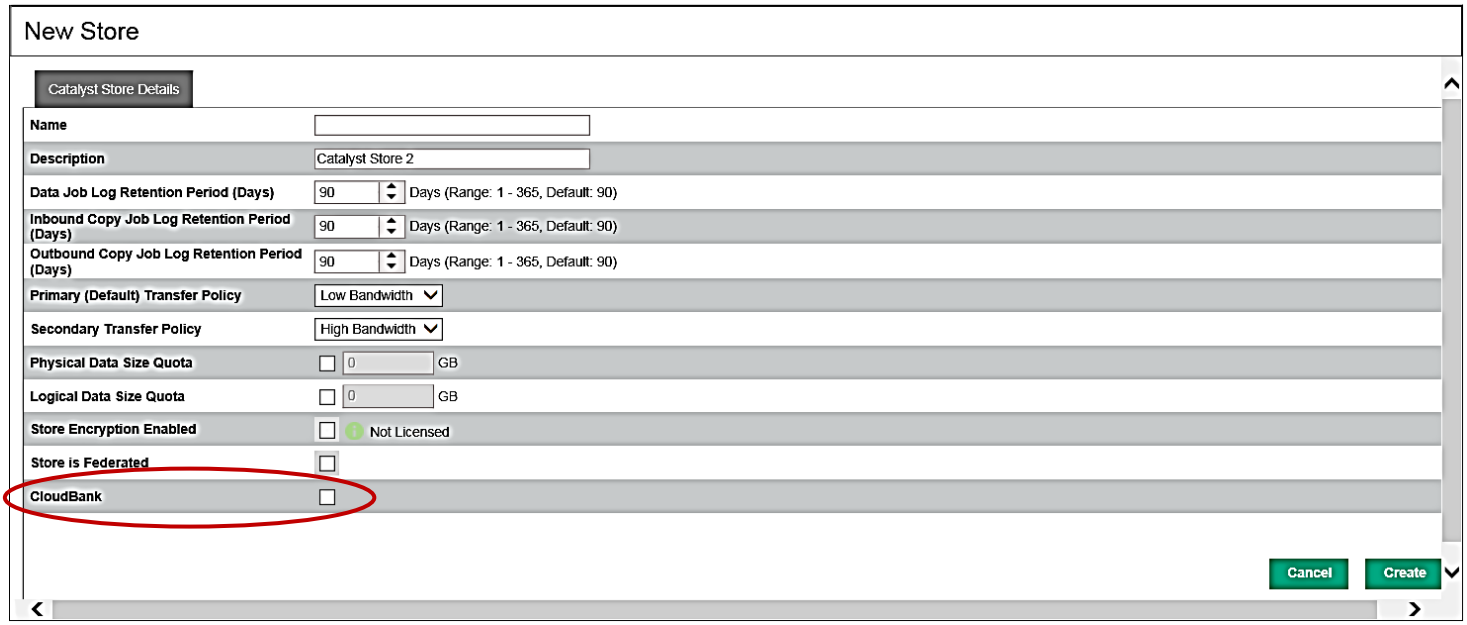

Figure 28. Creating a new StoreOnce Catalyst store

Checking **CloudBank** adds the **Cloud Service Provider** field to the **New Store** panel, shown in Figure 30. Notice in Figure 28 that this HPE StoreOnce unit is not licensed for Store Encryption. In this case, selecting the HPE Cloud Bank Storage feature presented a Warning panel, shown in Figure 29, advising you that HPE recommends enabling encryption with HPE Cloud Bank Storage Catalyst Stores. You must acknowledge this warning before continuing.

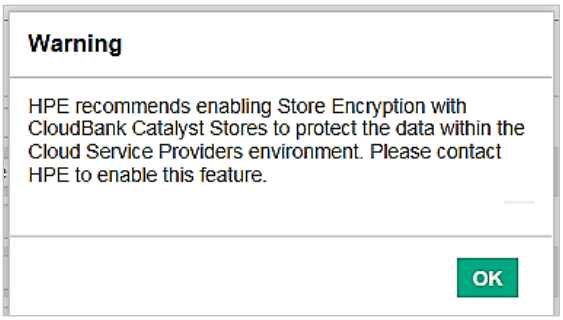

Figure 29. HPE recommends that HPE Cloud Bank Storage Catalyst Stores be encrypted

The Cloud Service Provider field shown in Figure 30 is a pull-down menu listing the HPE StoreOnce supported cloud providers.

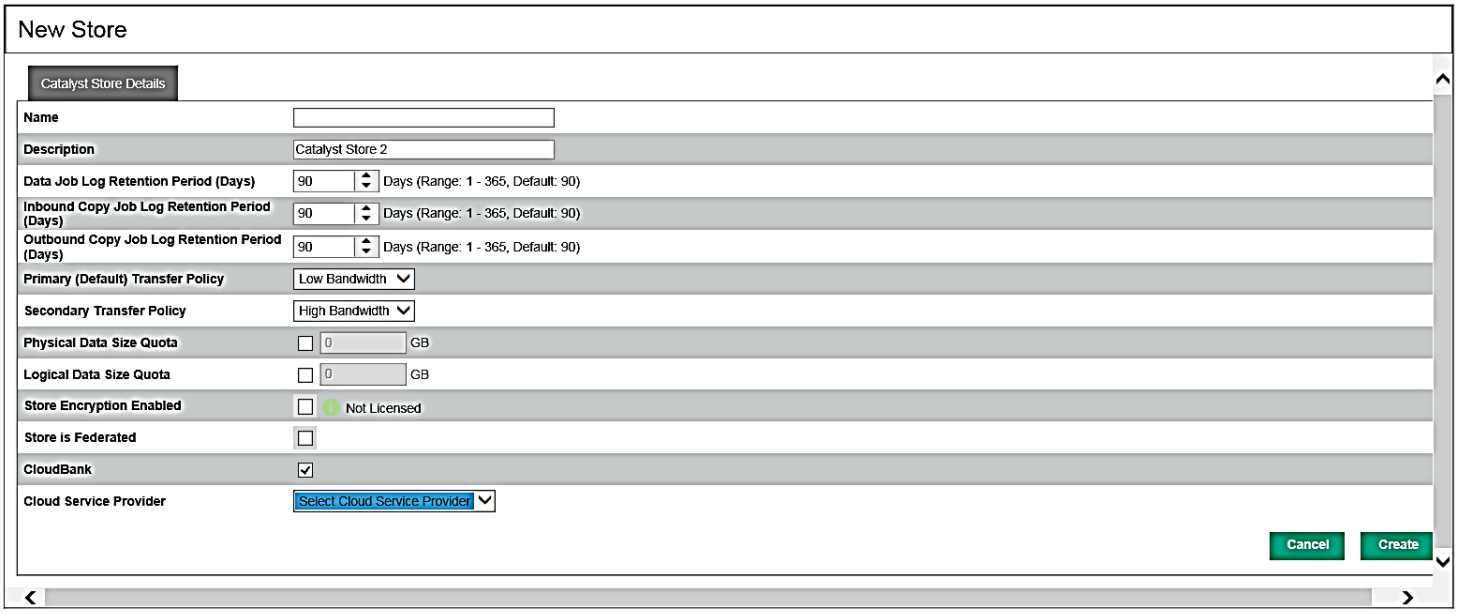

Figure 30. Selecting the Cloud Service Provider for this HPE Cloud Bank Storage store

Select **Scality** from the pull-down list. This adds the following five lines at the bottom of the New Store panel (Figure 31).

- Access key
- Secret key
- Host
- Port
- Bucket Name

The access key and secret key were created at the time the Scality S3 Connector was configured and they are the same as entered in the Add Storage Server panel (Figure 17) if you are using the same Scality S3 Connector service host.

The Host field entry must include the `http://` prefix. For example, using the same service host as in Figure 16, the Host entry would be `http://10.1.6.225`.

The default port is 443. This must be changed to port **80** for http connection.

The **Bucket Name** should follow the same naming conventions as given in the Create Buckets screen of the Disk Pool wizard (Figure 21).

Important

Unlike NetBackup, which creates the bucket during configuration of the storage server, for HPE Cloud Bank Storage Catalyst stores, the bucket name you provide must have already been created.

Figure 31 shows the completed entries for adding access to the Scality S3 Connector for the new HPE Cloud Bank Storage Catalyst store named `Scality-NBU-CloudBank`.

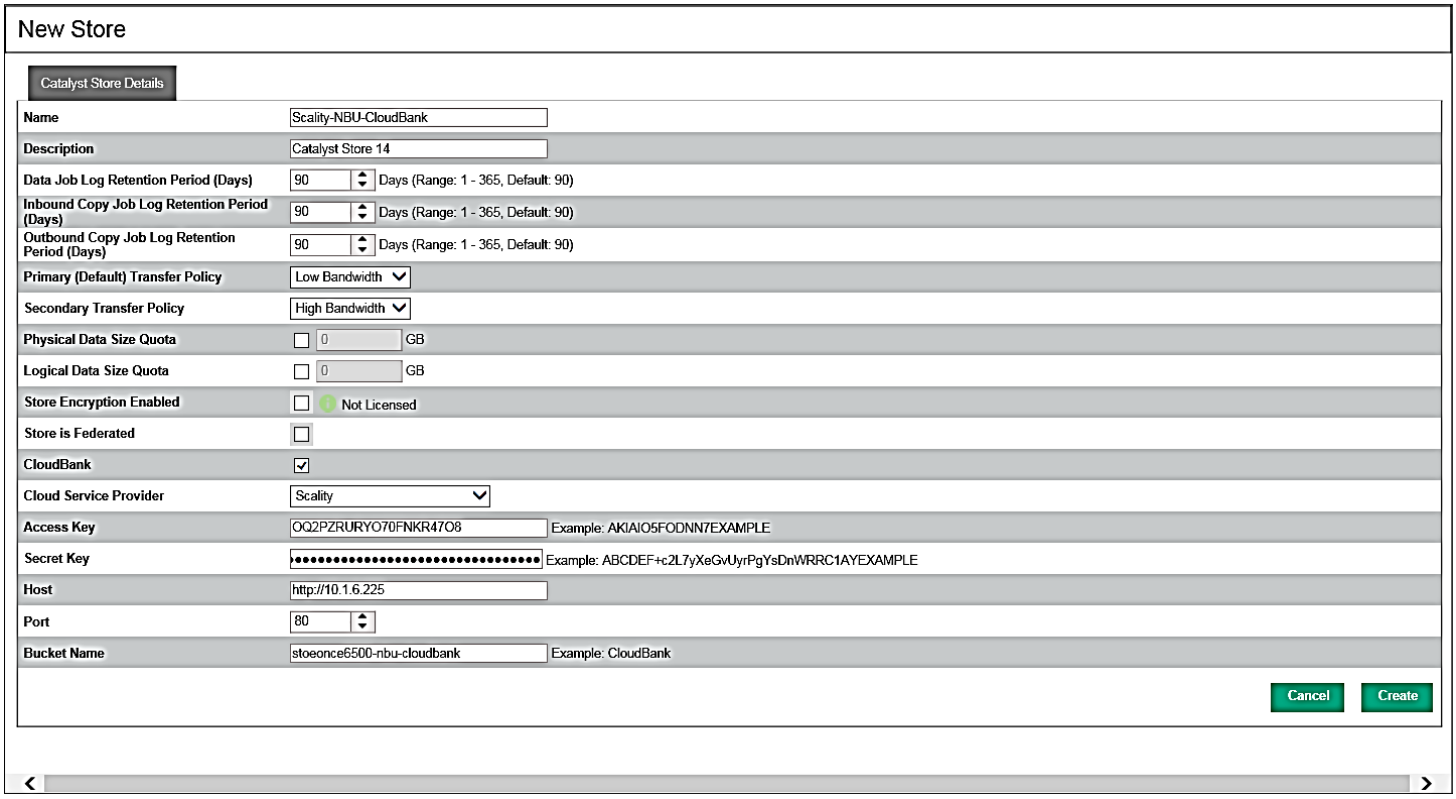

Figure 31. Adding Scality S3 Connector information

Click **Create** to complete creating the new store. The HPE StoreOnce validates the connection to the Scality S3 Connector using the credentials provided.

Creating a NetBackup storage server for the HPE Cloud Bank Storage Catalyst Store

Creating a storage server based on the HPE Cloud Bank Storage Catalyst Store follows the same procedure used to create a storage server based on a regular Catalyst store. From the NetBackup Administration Console, select the Disk Storage Servers Configuration wizard (Figure 13) and choose **OpenStorage** as the disk storage type. One of the first steps is to specify the Storage server type. Enter **hp-StoreOnceCatalyst** in this field, as shown in Figure 32. Note that the only media servers available in the pull-down list are those media servers that have the HPE StoreOnce Catalyst NetBackup OST plugin already installed.

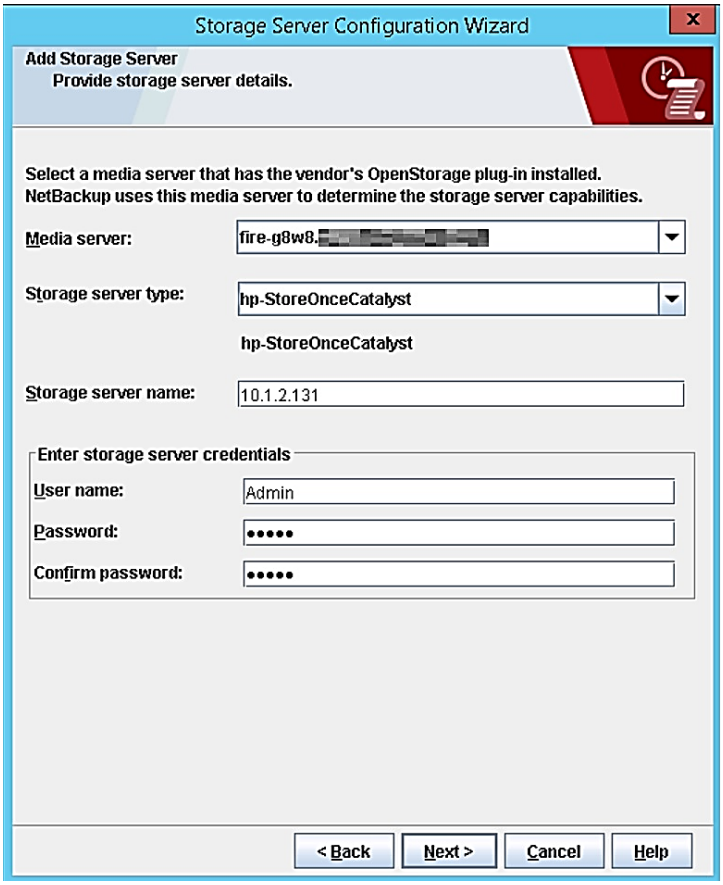

Figure 32. Adding an OpenStorage storage server of type **hp-StoreOnceCatalyst**

The wizard continues to the Disk Pool Configuration wizard shown in Figure 33. The Volume Name panel includes the names of all the Catalyst Stores discovered on the selected HPE StoreOnce storage server. In Figure 33, you see the Catalyst store name `Scality-NBU-CloudBank`, which was created previously (Figure 31).

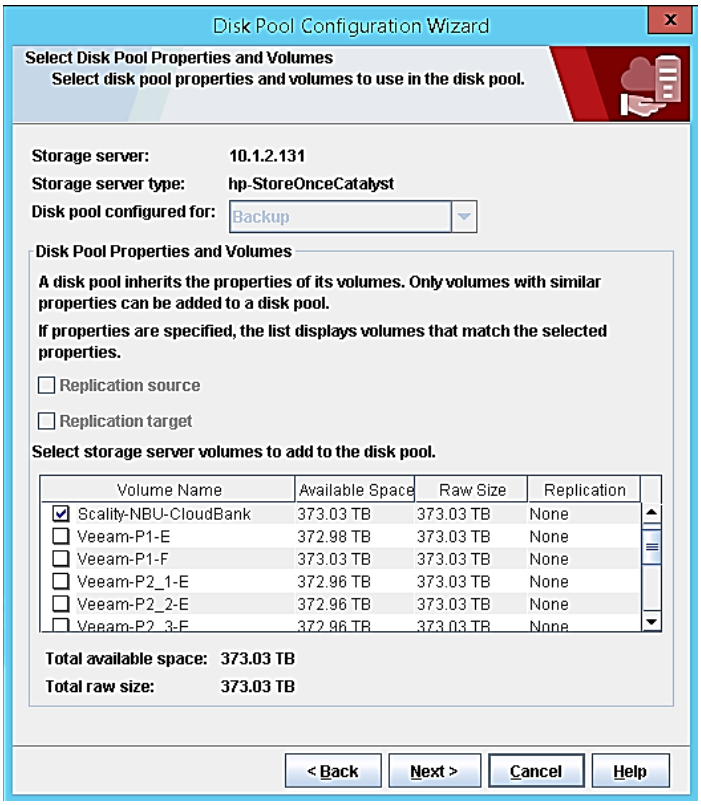

Figure 33. Selecting the HPE Cloud Bank Storage Catalyst Store as the Disk Pool volume

Continue with the wizard to complete the creation of the storage unit.

Creating a NetBackup Storage Lifecycle Policy

A Storage Lifecycle Policy defines the storage units, which will be used in a combined backup/duplication operation. When you create the Storage Lifecycle, you give it a name and then do the following:

1. Add the name of the storage unit that will be the target of the backup operation.
2. Add a second storage unit to the policy.

The second unit will be the target of the duplication (copy) operation. The source of the duplication operation is the backup operation's storage unit. You have the option to postpone creation of the copy until the source copy is about to expire. Otherwise, the duplication operation is launched after the successful completion of the backup.

Figure 34 shows the settings of a Storage Lifecycle Policy named `StoreOnceStore-StoreOnceCloudBank` with backup operations directed to the storage unit named `StoreOnce` (normal StoreOnce Catalyst Store) and duplication operations directed to the storage unit named `StoreOnce-CloudBank-stu` (StoreOnce Catalyst Cloud Bank Storage store).

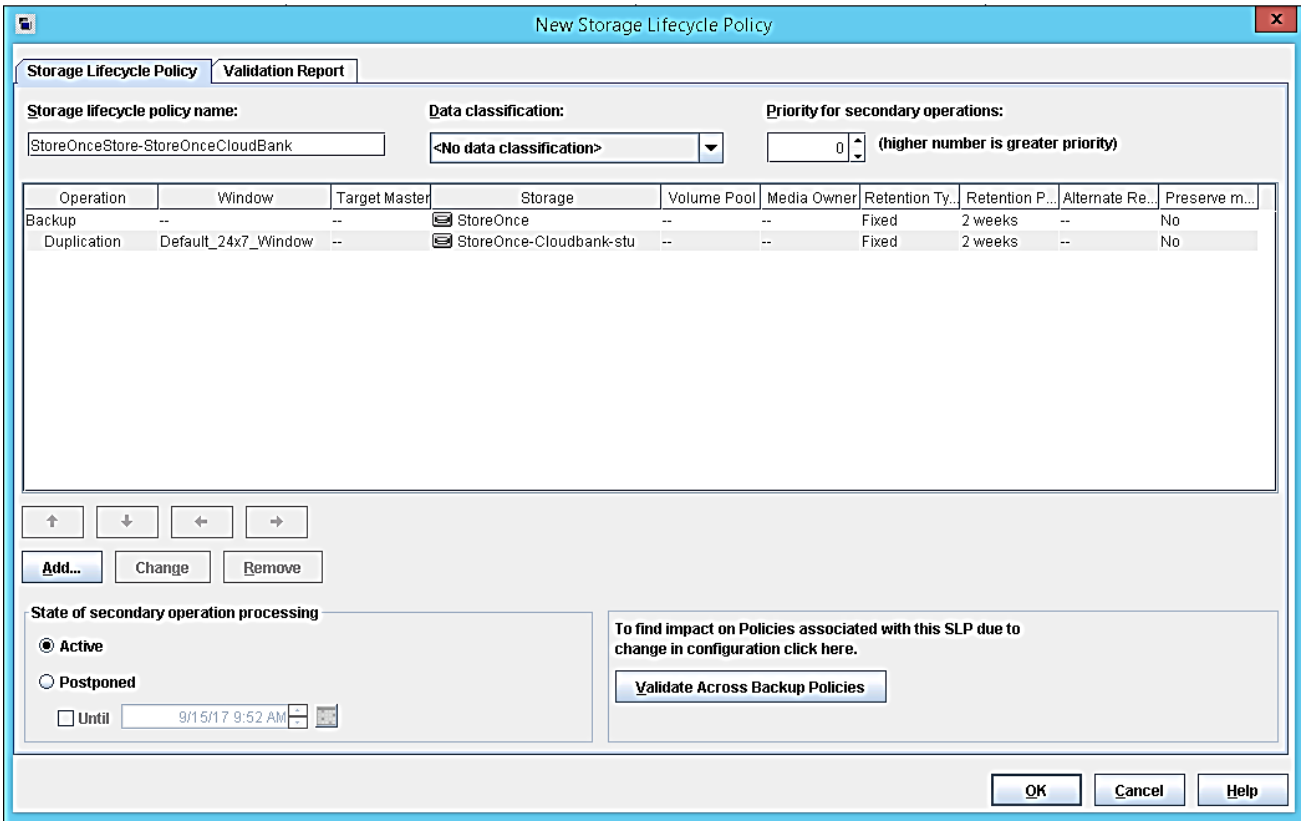

Figure 34. Storage Lifecycle policy using HPE Catalyst Store and HPE Cloud Bank Catalyst store

Creating a NetBackup Policy to use the Storage Lifecycle Policy

The Storage Lifecycle Policy only specifies the storage units to be used in a combined backup/duplication operation. It does not specify any of the parameters of the backup job itself; that is the function of a NetBackup Policy. A NetBackup Policy specifies the attributes, schedule, client server, and backup selection components of the backup portion of the combined backup/duplication operation. One of the key attributes in any policy is the selection of the policy storage. To launch a combined backup/duplication operation, a defined Storage Lifecycle Policy must be specified as the policy storage. Figure 35 shows the Policy storage pull-down menu The Storage Lifecycle Policy named `StoreOnceStore-StoreOnceCloudBank` is highlighted. By specifying the Storage Lifecycle Policy in the Policy storage attribute of the policy definition, backups will be directed to the HPE StoreOnce Catalyst store and the HPE StoreOnce will copy the backup sets to the HPE Cloud Bank Storage store.

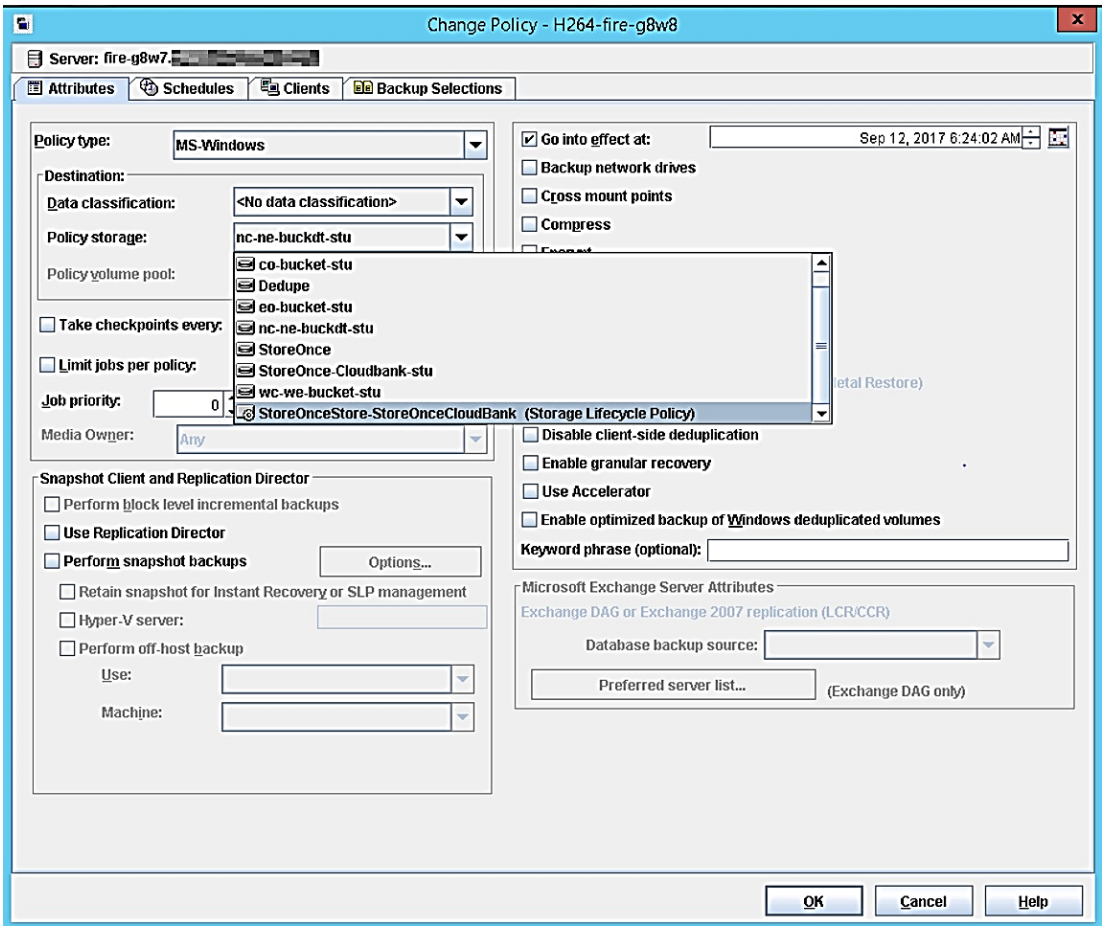

Figure 35. Choosing a Storage Lifecycle Policy as the Policy storage attribute of a backup policy

The policy is now complete and can be used in scheduled or manual backup operations. When the policy is launched, the NetBackup Activity Monitor displays **Backup** as the operation type during the backup of the selected data and displays **Duplication** when the copy operation commences.

Resources and additional links

HPE Storage
hpe.com/storage

HPE Apollo 4000 Systems
hpe.com/us/en/servers/hpc-apollo-4000.html

HPE Scalable Object Storage with Scality RING
hpe.com/storage/scalableobject

HPE Scalable Object Storage with Scality RING on HPE Apollo 4510 Gen10 technical white paper
hpe.com/h20195/V2/Getdocument.aspx?docname=a00026022enw

HPE Data Availability, Protection, and Retention Compatibility Matrix
support.hpe.com/hpsc/doc/public/display?docId=emr_na-c04616269

HPE Cloud Bank Storage: Data Protection Solution You Can Bank On
community.hpe.com/t5/Around-the-Storage-Block/HPE-Cloud-Bank-Storage-A-Data-Protection-Solution-You-Can-Bank/ba-p/6965903

To identify storage system configuration specifications and compatibility information, go to
h20272.www2.hpe.com/spock

For more information on Scality RING, go to scality.com

For more information on Commvault, go to commvault.com

For more information on IBM Spectrum Protect, go to
ibm.com/us-en/marketplace/data-protection-and-recovery

To access the Veritas NetBackup Compatibility List, go to
netbackup.com/compatibility

HPE Pointnext Advisory and Transformation Services
hpe.com/us/en/services/consulting.html

To help us improve our documents, please provide feedback at hpe.com/contact/feedback.

Learn more at

hpe.com/storage/scalableobject

Sign up for updates

a00038287enw, April 2018, Rev. 1