IBM Spectrum Protect

In-the-Cloud Deployment Guidelines with IBM Cloud

Document version 1.2

James Damgar

IBM Spectrum Protect Performance Evaluation

IBM

CONTENTS

List of Figures

List of Tables

Introduction

1.1 Purpose of this Paper

This paper introduces the possibilities for deploying IBM Spectrum Protect™ on an **IBM Cloud**™ **bare metal server** computing system. You can use the configurations that are presented here as a starting point for deploying a large, medium, small, or extra-small system, similar to those defined in the IBM Spectrum Protect Blueprints. With the goal of achieving a target daily ingestion rate (corresponding to a large, medium, small, or extra-small deployment), configuration possibilities are offered so that you can get a sense of the relative CPU, memory, disk, and network capabilities that are needed to satisfy requirements. In addition, an overview of options for meeting the requirements is provided. The current IBM Cloud offerings for bare metal servers represent a wide gamut of available options, which are appropriate for different workloads. The availability of options depends, in part, on the IBM Cloud data center being considered and whether servers are provisioned on an hourly or monthly basis. Certain systems might be sufficient in some system resource areas while lacking in others. You must recognize where system bottlenecks might arise that could limit IBM Spectrum Protect capability.

Use this paper as a **starting point for guidance** about where and how to deploy an instance of the IBM Spectrum Protect server on a dedicated IBM Cloud bare metal server for large, medium, and small deployment, or an IBM Cloud virtual server for extra-small solutions. This paper presents options for deploying IBM Spectrum Protect in two configurations:

- A configuration in which primary IBM Spectrum Protect backup-archive data is stored directly to cost-effective IBM Cloud Object Storage (hosted within IBM Cloud)
- A configuration in which several days of operational recovery data is kept on a (directory-container storage pool) disk tier for rapid recovery and older, inactive data is demoted to and preserved on IBM Cloud Object Storage. This option can prove cost effective for IBM Cloud bare metal servers.

The choice of architecture depends on the mixture of data recovery objectives and cost goals for a specific solution. Restore rates are generally slower for data in object storage than for data in localized block storage. However, object storage capacity costs are usually lower than costs for block disk, especially for cloud-hosted environments.

For the **direct-to-cloud** architectures, backup data is ingested directly into a **cloud-container storage pool** with a performant accelerator cache disk location tuned for a system's ingestion workload as the initial "landing spot" (for more information, see Sizing the Cloud Accelerator Cache). Data is then immediately, asynchronously transferred to object storage while further data is also ingested into the disk staging area (also known as *overlapped I/O*). The key consideration here is to determine the performance characteristics that the disk staging area must provide to allow for this mixed write-and-read behavior to ensure that ingestion targets are met. A *Cloud Cache and Object Storage Benchmarking* guide and "Cloud benchmarking tools" packages are provided along with this paper to assist in benchmarking both the cloud accelerator cache and object storage system from a prospective host server.

The **disk-to-cloud** tiering architectures make use of IBM Spectrum Protect **storage rules** to demote data from a small directory-container storage pool (disk tier) to a cloud-container storage pool. Backup data is initially ingested into a directory-container storage pool and later a portion of this data is moved asynchronously to a cloud-container storage pool. This can be done with either age-based tiering (available as of IBM Spectrum Protect Version 8.1.3) or tiering by backup state (available as of IBM Spectrum Protect V8.1.6). With IBM Spectrum Protect V8.1.6, a combination of storage rules and storage subrules can be used to facilitate more granular tiering behavior between the disk and object storage tiers, allowing for flexibility and filtering by node and node file space, for example. Some guidance is given in this paper to assist with determining whether tiering is suitable for your workload demands and characteristics.

1.2 Considerations for Disk-to-Cloud Tiering Versus Direct-to-Cloud Data Movement

The primary advantage of the **tiering** model is that operational recovery data can be preserved on a localized, fast disk tier for rapid recovery while older copies of data or data intended for long-term retention can be demoted to object storage, which is typically more affordable. The tiering model can also be used as an alternative to the direct-to-cloud model with a relatively small disk tier footprint (not strictly for operational recovery purposes). When the `TIERDELAY` parameter is set to 0, age-based tiering can be used to tier each day's worth of ingested client data after it is ingested (after the backup operation is completed). In this case, potentially less expensive disk can be provisioned for use by the small disk container pool tier because no ingest and cloud transfer input/output (I/O) operations occur in parallel. Tiering can be run serially after the completion of data ingestion during scheduled windows with less or no contention for this disk; the disk area can be cleared in preparation for the next day's ingestion.

The same ingestion targets can be satisfied with the disk-to-cloud tiering model as with the direct-to-cloud model, assuming that the direct-to-cloud approach makes use of an accelerator cache and overlapped data ingestion.

Restriction: To implement cloud tiering, you must provision enough disk space to hold a full day's daily ingestion (plus some buffer) to avoid failed backup operations. The same underlying disk technology can be used in both cases. If, however, you plan to use disk-to-cloud tiering to hold one or more days' worth of operational recovery data within a container pool disk tier, the instance disk capacity might have to be much greater, with the caveat that a slower-performing disk might be sufficient for this case. In all cases, you must understand the ingestion targets (after data deduplication and compression) to determine a daily disk capacity for a transient disk case. Meanwhile, operational recovery requirements in terms of the number of days' worth of recovery data (after deduplication and compression) should be determined to further size a disk container pool with tiering to cloud if necessary.

With the **direct-to-cloud** model, you can minimize local block storage capacity. This is an advantage because local block storage can be cost prohibitive in cloud-hosted environments. For example, consider an environment with IBM Cloud virtual servers where Portable SAN Storage Volumes (PSV) are the main option. When you store primary backup data to object storage (with only a small, transient amount of cloud accelerator disk cache required during ingest), you can achieve cost-effective object storage.

1.2.1 Cloud Accelerator Cache Considerations

Beginning with IBM Spectrum Protect V8.1.2, data ingestion from clients is throttled if the accelerator cache area is near capacity. This feature makes it possible for this disk cache location to be **underprovisioned** from a capacity standpoint in that the disk cache location does not have be sized large enough to hold a full day's worth of deduplicated and compressed data. However, the accelerator disk still must be performant enough in terms of input/output operations per second (IOPS) so that client data ingestion and replication target activity can be completed in a timely manner. In the end, you have to compare costs to determine whether larger capacity, less-expensive disk with tiering has an advantage over a direct-to-cloud cache model for a given environment, ingestion rate, and recovery objective.

Restriction: If you plan to use the direct-to-cloud ingestion model, the cloud accelerator cache should be sized large enough to hold at least two times the largest front-end object being ingested. For example, if a 512 GB object is to be ingested directly into a cloud-container storage pool, the cloud accelerator cache should be at least 1 TB in size. Similarly, if 5 client sessions will be backing up 100 GB files each at the same time, the cloud accelerator cache should be sized to at least 1000 GB (5 clients x 100 GB files x 2). This is because the IBM Spectrum Protect server will attempt to "reserve" space in the cloud accelerator cache for in-flight ingestion until those ingested objects are completely finished and their database transactions are committed to the server. By default, this processing assumes no deduplication or compression savings and attempts to reserve the total front-end amount of data to ensure sufficient storage capacity.

Beginning with IBM Spectrum Protect V8.1.6, a server option can be used to influence this behavior. The `PreallocReductionRate` server option can be used to give the server a "hint" about the expected reduction ratio for ingested data and cause the server to reserve less physical space in the container storage pool. For example, setting this option to 5 will cause the server to assume a 5:1 data reduction rate for front-end to back-end data so that only 1 unit of back-end space will be reserved for 5 units of front-end protected data. This option can range from 1 (the default, no reduction) to 8 (an 8:1 assumed reduction). Use this option only when a smaller cloud accelerator cache is desired and data reduction rates are certain. If the storage pool has inadequate space, backup failures can result.

1.2.2 Workload Limitations and Considerations with Tiering

Not all client workloads are suitable for a disk-to-cloud tiering model. Age-based tiering (as of IBM Spectrum Protect V8.1.3) allows for the demotion of *backup* objects that are older than a specified age. Inactive backup generations that are older than the specified age are transitioned to object storage. State-based tiering (as of IBM Spectrum Protect V8.1.6) allows for the demotion of *backup* objects that are inactive within the server. Active backup objects are preserved on the disk tier, while inactive copies of backup objects are transitioned to object storage.

Disk-to-cloud tiering is **suitable** for client workloads that have **low** data deduplication rates (backup generations differ greatly). In this case, data is highly unique between backup operations. When a backup generation is tiered to object storage, the deduplicated extents (chunks) that make up that object have their references decremented on the source directory-container storage pool. In this case, reference counts are likely to be low and more deduplicated extents are likely to be removed from the disk tier as objects are tiered and space is released.

Disk-to-cloud tiering **may not be suitable** for client workloads that have a **high** data deduplication rate. In this case, data is not very unique between backup generations and many shared deduplicated extents are referenced by multiple object generations. Even though an object can be tiered by a storage tiering rule, because the object shares many extents with other objects (which might still be active), a large proportion of the object's data will not be removed from the disk tier (although it will be copied to the object storage tier).

The following figures illustrate how data movement with disk-to-cloud tiering can occur. Figure 1 depicts a scenario in which multiple versions of three backup objects (A, B, and C) have been ingested and are stored in a directory-container storage pool on disk. Dotted lines represent references to deduplicated extents (colored, numbered boxes). With the tier-by-state option, the inactive object copies highlighted within the gray rectangle would be tiered to a cloud-container storage pool.

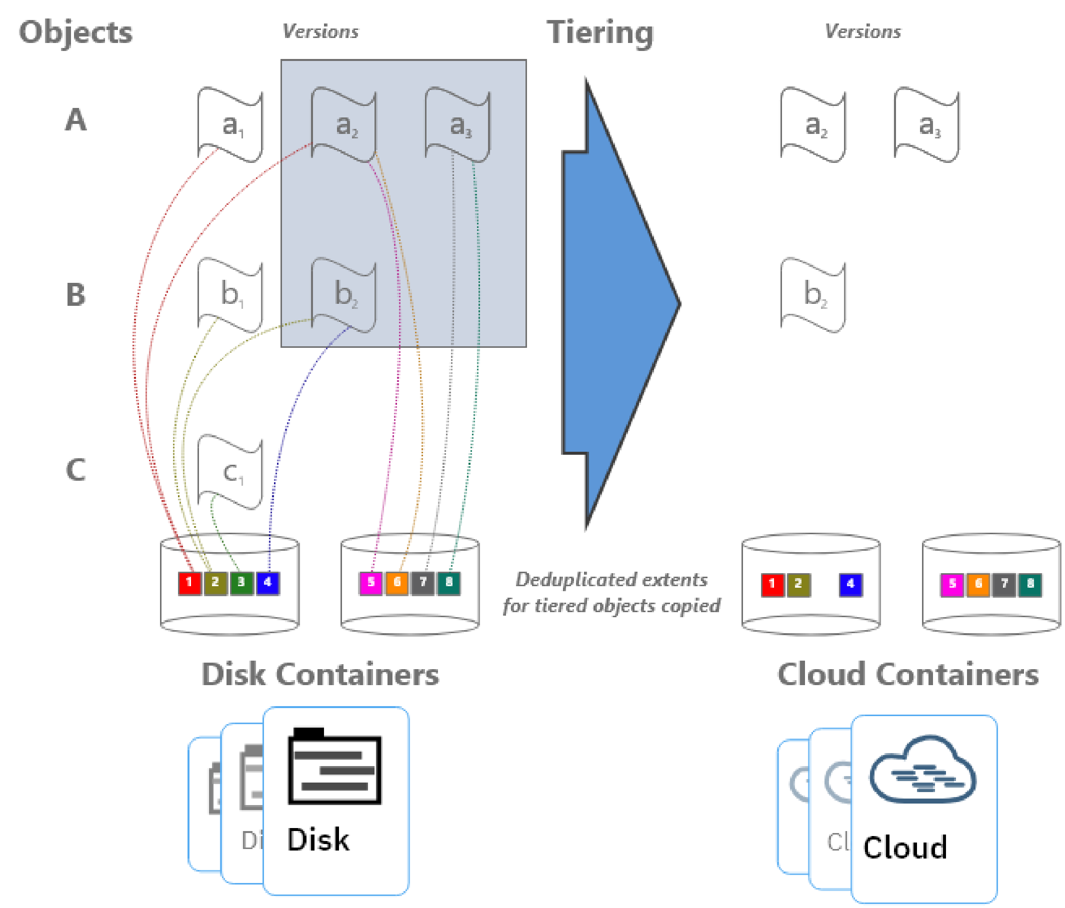


Figure 1: Disk-to-cloud tiering, before and after

Figure 2 depicts the situation after tiering is completed and the `REUSEDELAY` parameter value of the source directory-container storage pool is exceeded (so that deduplicated extent removal for extents with zero reference count can occur).

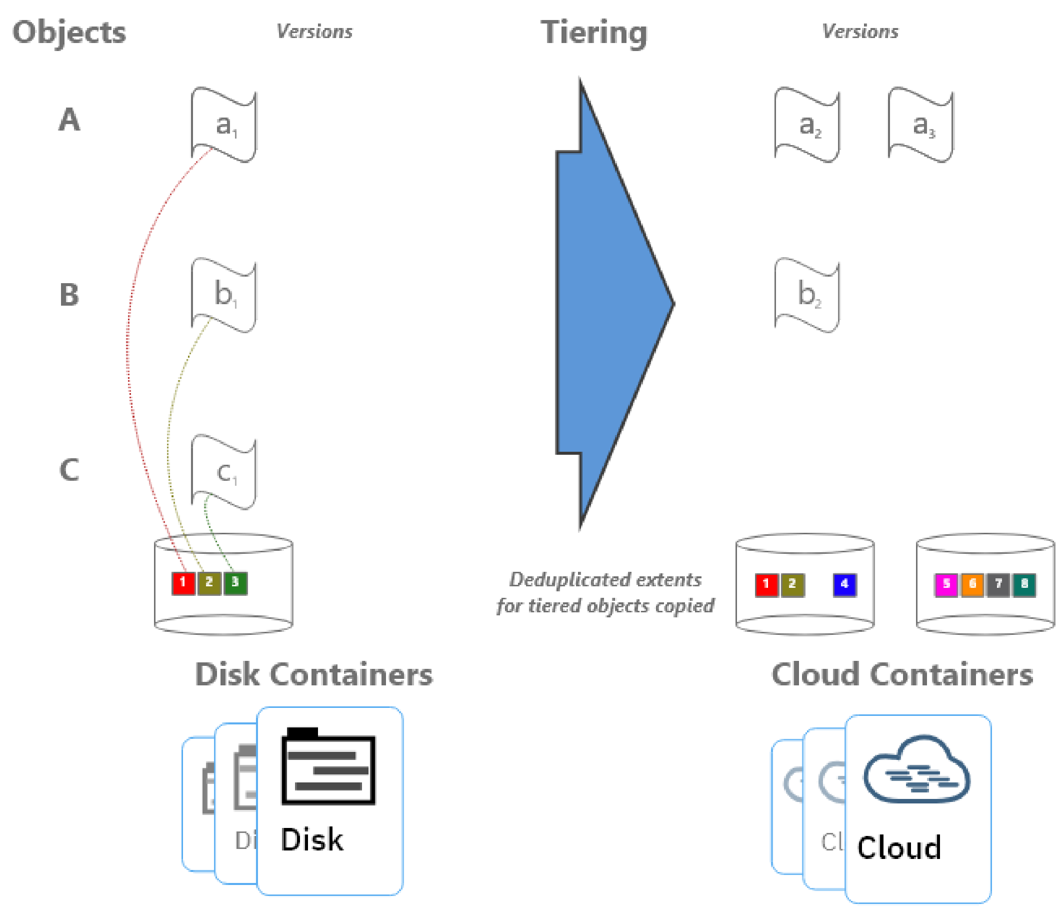


Figure 2: Disk-to-cloud tiering, after tiering

Notice that deduplicated extents 1 and 2 remain on disk even after tiering and extent cleanup have occurred. This is due to the fact that those extents are shared between the active and inactive backup copies. If many deduplicated extents are shared by objects (a high duplicate data rate with high data deduplication ratios), it is more likely that data will remain on disk, even after backup objects have been tiered at an IBM Spectrum Protect inventory level. Keep this factor in mind when you consider a disk-to-cloud tiering model and when you size an environment.

For workloads that deduplicate well from day to day, there will be many shared extents across backup and archive generations and a smaller capacity footprint on tiered object storage as a result because these backup and archive generations will also share many extents in the cloud-container storage pool. For workloads that deduplicate poorly day to day (highly unique data change each day), there will be few shared extents across backup and archive generations and potentially a larger capacity footprint on tiered object storage because these backup and archive generations will each point to (more) unique data in the cloud-container storage pool.

If the primary motivation for using disk-to-cloud tiering is rapid recovery of operational recovery data, a tiering model might provide the best approach. You must understand the nature of the client workload to accurately size the directory-container storage pool on disk.

1.3 Cloud Deployment Patterns

The configurations described in this paper can be used as starting points in situations where the IBM Spectrum Protect cloud instance will be a **primary server and in situations where it is used as a replication target**. In scenarios where the IBM Cloud based instance is a replication target, adequate "public" network capability might be sufficient to satisfy the replication throughput requirements of a solution. IBM Cloud Direct Link is a comprehensive service that includes the ability to establish dedicated links ranging from 50 Mbps to 10 Gbps with partner providers between an on-premises data center and IBM Cloud hosted resources. Such links can help to facilitate efficient IBM Spectrum Protect replication or client backup processing from clients or peer servers outside of the IBM Cloud private network.

Generally, IBM Spectrum Protect deployments making use of cloud-based object storage will align with one of the following three patterns:

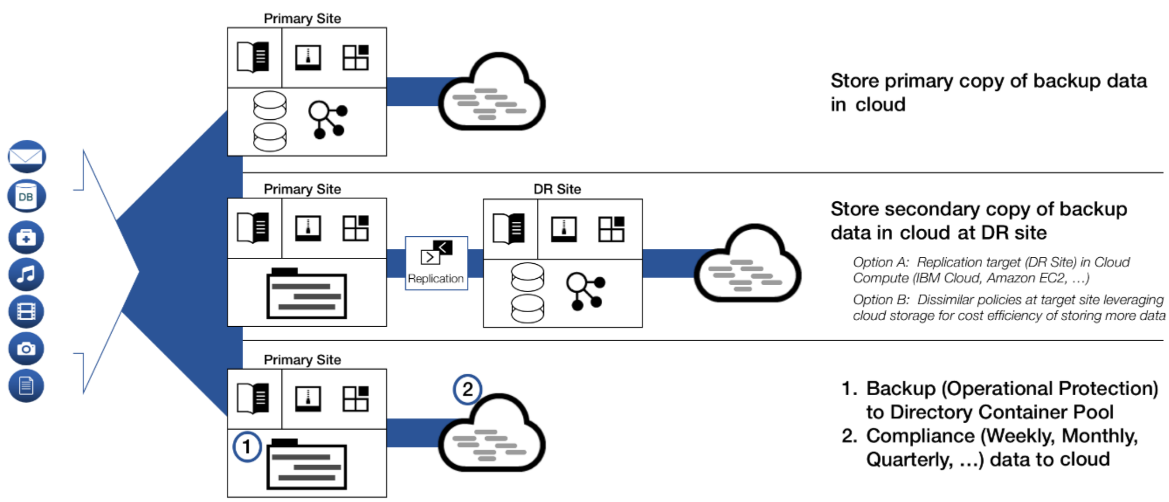


Figure 3: Deployment patterns

In the figure, the **first** deployment pattern could involve an IBM Spectrum Protect server that is installed on premises or within an IBM Cloud server, with primary backup data landing in object storage immediately. The positioning of the IBM Spectrum Protect server in relationship to clients could be one critical decision point when you consider whether to have a server instance on premises or hosted in IBM Cloud, with further considerations involving whether IBM Cloud Direct Link is used. This pattern could involve use of a direct-to-cloud architecture with accelerator cache or a small disk container pool with immediate tiering to a second cloud-container storage pool without accelerator cache.

The **second** deployment pattern would make use of IBM Cloud Object Storage at the secondary disaster recovery (DR) site. This DR server could be installed at an on-premises site or on an IBM Cloud server. In the latter case, sufficient wide area network (WAN) bandwidth between the primary and secondary sites is required for acceptable performance. Much like the first deployment pattern, here the IBM Spectrum Protect server at the DR site could make use of a direct-to-cloud topology with a cloud pool featuring accelerator cache, or it could use a small disk container pool landing spot with immediate tiering to a cloud pool backed by object storage.

The **third** deployment pattern features specific use of disk-to-cloud tiering to allow for operational recovery data to reside on faster performing disk storage. This could involve age-based tiering (available with IBM Spectrum Protect V8.1.3 and later) or state-based tiering (available with IBM Spectrum Protect V8.1.6 and later), or a mixture of the two approaches tailored for a specific purpose. Data that is older, archived, or both would be tiered to cloud-based object storage after a specified number of days or by its state (active or inactive) within the server. This deployment also could be configured at an on-premises site or within an IBM Cloud server. However, the additional cost of having a larger capacity disk container pool should be factored into cost estimates with an in-the-cloud solution.

A **combination** of approaches is also possible within the same deployment. For example, a cloud-container storage pool could be configured with accelerator cache disk and made to take in long-term retention or compliance archives. A directory-container storage pool could be configured as a disk tier for normal backups, and a tiering relationship could be set up so that operational recovery data (for example, backups from the previous 7 days) is kept on this disk tier, while older data is demoted to the same cloud-container storage pool. The same cloud-container storage pool can be a direct backup target and a tiering target. However, if the pool is a direct target of a backup-archive client, the pool must be configured with accelerator cache disk.

1.4 Cloud Environment Considerations

For IBM Spectrum Protect solutions in the **IBM Cloud**, generally a **bare metal server** rather than a virtual server will be needed to satisfy Ethernet network requirements. Network capability in **excess of 1 Gbps** to one of the IBM Cloud Object Storage endpoints accessible over the private IBM Cloud network for the cloud-container storage pool is required to achieve large, medium, or small Blueprint-level ingestion rates. The selection of bare metal servers can vary based on the desired IBM Cloud data center and whether monthly or hourly provisioning is desired. Various options can be used to satisfy IBM Spectrum Protect requirements and to provide adequate flexibility for tuning server selections. Ensure that you select bare metal server offerings that include a large enough chassis to support the required number of **internal disks** for IBM Spectrum Protect. In this document, systems with either 24 or 36 internal disks are outlined. For the extra-small server option, IBM Cloud virtual servers are an appropriate choice. IBM Cloud virtual servers can have a multitenant architecture (for greatest cost savings) or a single-tenant (dedicated) architecture and can be provisioned with hourly, monthly, or yearly billing terms.

The selection of an IBM Cloud bare metal server is a significant choice in that moving to another server type after deployment would require a complete rebuild. The large, medium, and small solutions outlined here involving IBM Cloud make use of physical server deployments with all-internal disk configurations (no attached IBM Cloud Block disk is used). If the desired IBM Spectrum Protect server sizing is initially unclear, or the server requirements might change over time, and you can collocate other, non-IBM Spectrum Protect workloads in IBM Cloud as well, you could potentially provision a larger bare metal server and install hypervisor virtualization software on the host. In this way, you can provide flexibility in provisioning CPU and memory resources to an IBM Spectrum Protect virtual machine, which could be altered later as needs change. However, this paper addresses only installations of IBM Spectrum Protect on bare metal servers with no hypervisor and a single operating system.

1.4.1 The Importance of Adequate Sizing

Ingested backup data reaching the cloud accelerator cache or the initial disk container pool tier requires the use of block storage allocated to the cloud server. IBM Spectrum Protect database activity also uses some level of throughput and elevated I/O operations during workload processing. Therefore, disk **I/O capability** and server-to-disk throughput considerations are paramount when deploying an IBM Spectrum Protect instance. To help achieve the required performance level and to reduce cost, internal, in-chassis JBOD disks and redundant arrays of independent disks (RAID) are used with large, medium, and small IBM Cloud systems. With a final ingestion point on object storage via a cloud-container storage pool, the **Ethernet capability** of the server and the nature of the network between the server and the IBM Cloud Object Storage endpoint should be kept in mind. In addition, you must consider how the front-end client data workload is deduplicated and compressed into a back-end storage quantity.

A lack of adequately performing disks can lead to bottlenecks in the IBM Spectrum Protect server's database operations. Certain IBM Cloud bare metal servers might have, or be configured with, limited throughput over Ethernet, and this limitation could hamper ingestion and restore throughput with IBM Cloud Object Storage. During the planning phase, consider how the ingested data will be **reduced via data deduplication and compression** at the back-end storage location. These factors will help you estimate how much back-end data must be moved within a certain time window (measured in hours) and can help predict the throughput (megabytes per second or terabytes per hour) that the Ethernet network and object storage endpoint require to satisfy ingestion requirements. Generally, **10 Gbps** Ethernet capability to private IBM Cloud Object Storage endpoints is required for large, medium, or small Blueprint ingestion targets while 1 Gbps is sufficient for extra-small targets.

Beginning with IBM Spectrum Protect V8.1.3, the server automatically throttles client backup operations if the cloud accelerator cache portion of a cloud-container storage pool is nearing full capacity. As a result, it is not mandatory to configure cloud accelerator disk cache space that would be large enough to hold a full day's worth of backups (after data deduplication and compression). However, disk benchmarks should be run to ensure that the anticipated back-end workload that an IBM Spectrum Protect server is expected to support will not result in this disk location being the primary bottleneck of the system (see Disk Benchmarking). In practice, any planned deployment should be validated to ensure that it will meet performance requirements.

Finally, with IBM Cloud bare metal servers, the availability of certain servers might be limited by the data center location and whether hourly or monthly provisioning is desired. Server options can also change over time by data center. Consult the latest list of available bare metal servers at your desired data center for current information.

With IBM Cloud virtual servers, virtual CPU (vCPU) and RAM capacity can vary. Certain models of virtual servers allow only for locally-attached disks while others feature the option of portable SAN storage volumes (PSVs). Locally attached disk size generally increases with the relative size of the virtual server (vCPU, RAM) while SAN-attached volumes are available in a range of capacities. IBM Cloud virtual servers can be a cost-effective option for smaller server deployments. An Ethernet network limitation of 1 Gbps for virtual servers can make it difficult to achieve small Blueprint or larger daily ingest targets.

1.4.2 Linux Logical Volume Manager (LVM)

The described reference architectures use either the Red Hat Enterprise Linux or Ubuntu Linux operating systems. For the **disk-to-cloud tiering** configurations, the preferred method for provisioning storage volumes from the shared database backup, archive log, and directory-container storage pool RAID 6 disk arrays for large, medium, and small options is to use the **Linux Logical Volume Manager (LVM)**. Each RAID 6 array (one array for small and medium systems and two for large systems) is presented to the operating system as a single physical disk. Create a single volume group for each RAID 6 array. Then, use the created volume groups for database backup, the IBM Db2® archive log, and the directory-container storage pool disk. Because only one physical disk (representing a RAID 6 array volume) is used per volume group, striping information is not needed. For more information, see Disk Setup Commands for Linux Deployments.

1.5 References to Physical IBM Spectrum Protect Blueprints

Throughout this paper, the server specifications in the *IBM Spectrum Protect Blueprint and Server Automated Configuration for Linux x86 Version 4.1* document (also known as an IBM Spectrum Protect Blueprint) are referenced as targets for CPU and memory configurations matching small, medium, and large server builds. For more information about the Blueprints, see References [1]. The intention with the server builds outlined here is to provide systems capable enough from a CPU, memory, disk, and Ethernet point of view to approach Blueprint-level ingest capability. Although different instance types can be used to satisfy the same requirements, the disk specifications in particular should be noted in this document as guidance for those deploying environments of their own.

As a reference, the following table indicates the throughput, capacity, CPU, and memory targets for each of the referenced Blueprints. The values for total managed data and daily ingest data are for the block storage Blueprints. These ingestion targets assume an 8-hour backup window.

Table 1: IBM Spectrum Protect physical Blueprint targets (V4.1, Linux x86)

Sizing category	CPU	RAM memory	Total managed data (front end)	Daily ingest data (front end)
Small	16 cores	64 GB	60 TB – 240 TB	Up to 10 TB per day
Medium	20 cores	192 GB	360 TB – 1440 TB	10 – 30 TB per day
Large	44 cores	384 GB	1000 TB – 4000 TB	20 – 100 TB per day

Although not defined explicitly in the physical Blueprints, the extra-small cloud Blueprint systems target up to 10 TB or more of total managed (front-end) data with a daily ingestion rate of up to 1 TB, or more, per day.

1.6 Database Backup Capacity

The configurations in this document are provisioned with enough IBM Spectrum Protect **database backup disk** space to hold two days' worth of full database backups in the worst case (with the Db2 database consuming close to its resident capacity). This approach was taken to avoid excessive attached disk cost and for chassis space limitation reasons with IBM Cloud. The IBM Spectrum Protect server is presently incapable of storing database backups directly to object storage. To configure recovery protection for a longer period (for example, 7 – 10 days), the database backup disk space that is listed here might have to be increased. One possible option is to use larger capacity, serial attached technology attachment (SATA) volumes for database backup disks (8 TB SATA drives instead of 4 TB, for example). Some configurations presented here maintain available drive slots in the server chassis. The slots can be used for additional drives to increase the size of the database backup RAID 5 array during initial configuration, as another option. For the extra-small virtual server option, a larger portable SAN storage volume (PSV) could be provisioned for database backup and archive log purposes.

1.7 Server Maintenance Scheduling Considerations

The *IBM Spectrum Protect Blueprint and Server Automated Configuration for Linux x86 V4.1* document features a detailed breakdown of the procedure for setting up IBM Spectrum Protect server maintenance schedules (see References [1], Chapter 5). Use this information as a reference for establishing a maintenance schedule on cloud-hosted servers.

For an IBM Spectrum Protect server in IBM Cloud that is serving as a replication target, a replication window and schedule might have to be established. For servers using the direct-to-cloud model, where primary backup data is ingested directly into a cloud-container storage pool, a replication window might not be required if this server is not a replication target server because a cloud-container storage pool cannot be used as a replication source. In this case, redundancy requirements for the ingested client data can be met by the inherit redundancy of IBM Cloud Object Storage.

For an IBM Spectrum Protect server in IBM Cloud that is using the disk-to-cloud tiering model, a replication source strategy might be required. Replication can help to protect client data objects in the disk directory-container storage pool that have not yet been tiered (demoted) to object storage because only one copy of that data is present. To prevent excess data from being stored (pinned) to the disk tier, verify the following items:

- The source replication server (used for disk-to-cloud tiering) should be configured with a longer retention policy for the client data that is being replicated than does the replication target server.
- The retention policy that affects client node data on the target replication server should match the value of the `TIERDELAY` parameter of the storage rule responsible for tiering the same client node data on the source server.

In general, the server that is used for disk-to-cloud tiering – whether it be the source replication server or the target replication server – should be the server with the longer retention policy for the client nodes affected by the tiering storage rule.

1.8 Session Scalability by Blueprint Size

The *IBM Spectrum Protect Blueprint and Server Automated Configuration for Linux x86* document describes how to set the IBM Spectrum Protect server option `MAXSESSIONS`, based on Blueprint system size:

- Small system: 250 maximum simultaneous client sessions
- Medium system: 500 maximum simultaneous client sessions
- Large system: 1000 maximum simultaneous client sessions

(For more information about the Blueprint configurations, see References [1].)

The actual throughput scalability of an IBM Cloud based solution depends on many factors, including the configured disk capability and capacity of the system, the amount of CPU and memory resources available on the system, and the relative rate of data deduplication and compression for the data set that is ingested into the server. Larger objects, which feature a larger deduplicated extent size (for example, 250 - 350 KiB, or more) and which do not deduplicate or compress well (for example, less than 10%), will result in less database and computation (CPU) overhead, but will utilize more disk and network bandwidth. The logical reduction of front-end client data to the physical back-end data (which is actually written out and stored to disk and object storage) means that the disk, network, and object storage components will be stressed to a higher degree as client/server session counts increase. Memory usage by the IBM Spectrum Protect server might also be greater. As session counts increase, these components are likely to become a system bottleneck, limiting front-end throughput.

Objects that feature smaller, deduplicated extent sizes (for example, 60 - 100 KiB or similar) and that deduplicate and compress well (for example, 50% data deduplication with 50% compressibility) will result in less network, disk, and object storage bandwidth used, but will lead to more database and computation overhead to facilitate these data reduction operations. As session counts increase, CPU and database-related memory are likely to first become limiting factors for these data types. In general, the more successfully data can be deduplicated and compressed (and therefore the greater the data reduction from front-end to back-end data), the greater the number of feasible client sessions. The following table indicates a reasonable range of client session counts based on system size and data type, as well as the likely limiting factor for the system as the high end of the range is approached. For more information about these data types, see Throughput Measurements and Results.

Table 2: Preferred ranges of maximum values for client session counts

Cloud system size	**Large object, poor data deduplication and compression[1]**	**Large object, good data deduplication and compression[2]**	**Large object, small extent size, good data deduplication and compression[3]**	**Small object, poor data deduplication and compression[4]**
Extra small	10 - 50	25 - 50	10 - 50	10 - 50
Small	50 - 100	100 - 200	50 - 100	50 - 100
Medium	100 - 200	200 - 400	100 - 150	100 - 150
Large	300 - 400	400 - 500	150 - 200	150 - 200
Limiting factor at scale	Network, disk, object storage bandwidth, memory	CPU, memory or network, disk, object storage bandwidth	CPU, memory	CPU, memory

[1] This model uses 128 MiB objects, 250 - 350 KiB extents, and <10% data deduplication and compressibility. Full backup operations are used with pseudo random data or data that cannot be easily deduplicated or compressed. For example, this model can be applied to encrypted data.

[2] This model uses 128 MiB objects, 150 - 200 KiB extents, and 50% data deduplication and compressibility. For example, this model can be applied to virtual machine backups.

[3] This model uses 1 GiB objects, 60 - 100 KiB extents, and 50% data deduplication and compressibility. For example, this model can be applied to database image backups.

[4] This model uses 128 KiB objects and <10% data deduplication and compressibility. For example, this model can be applied to file server data and other small files or objects.

Often, a diminishing rate of return regarding throughput is experienced when 50 - 100 total client sessions are exceeded, regardless of data type. More sessions are possible and might be warranted, given the client schedule or other requirements. However, aggregate gains in total throughput of a single IBM Spectrum Protect instance might not be substantial past this point.

IBM Cloud Computing Configurations

IBM Cloud

You can deploy IBM Spectrum Protect in an **IBM Cloud** server. For an introduction to IBM Cloud resources, see IBM Cloud.

The following configurations serve as possible options for deploying IBM Spectrum Protect in an IBM Cloud server with the final destination of ingested data being either purely on public **IBM Cloud Object Storage** (for a direct-to-cloud variant) or with some operational recovery data on a fast-restoring disk tier, with data that is older, inactive, or both being demoted to IBM Cloud Object Storage for longer term retention (for a disk-to-cloud tiering variant). The large, medium, and small options provided here involve bare metal servers as opposed to virtual servers in order to avoid the Ethernet network constraints of virtual servers (see References [2]). A bandwidth exceeding 1 Gbps to object storage is necessary to reach Blueprint-level daily ingestion targets to object storage. For cost-effectiveness, an IBM Cloud virtual server is used for the extra-small option. Configurations in this document can be set up to use either the single-site IBM Cloud Object Storage **Regional** offering or the multisite **Cross Regional** offering for object storage using a **Standard** storage class.

IBM Cloud deployments have an advantage in that provisioned instances have access to an internal private IBM network providing access to IBM Cloud Object Storage. By using the closest, private domain Regional or Cross Regional object storage endpoints, as opposed to the normal public endpoints, you can allow for network traffic to bypass the public WAN and permit a user to save on cost by not having to pay the typical ingress and egress charges associated with IBM Cloud Object Storage data entering and leaving the IBM network.

The bare metal server configurations use **RAID** and hot spares for certain groups of disks. Bare metal servers require installation of internal disks within the server chassis rather than being SAN-attached (as would be the case with IBM Cloud Block Storage). RAID is included for a level of protection in case of physical disk outages.

For each small, medium, or large environment, two configurations are presented:

- The first configuration is intended for a direct-to-cloud, accelerator cache-backed strategy involving a small, high performing cache disk landing area housing incoming data that is quickly transmitted to object storage.
- The second configuration is intended for disk-to-cloud tiering, available in IBM Spectrum Protect V8.1.3 and later. In this case, a larger, SATA disk configuration is used to house a more sizeable disk tier, where operational recovery data of multiple days is stored.

For the extra-small environment, a direct-to-cloud configuration is featured.

Table 3: IBM Cloud, large configuration, direct-to-cloud model

Cloud component	**IBM Cloud component**	**Detailed description**	**Quantity**
Server and network	Intel® Xeon® E7-4850 v2 (bare metal server)	48-core* Intel Xeon CPU E7-4850 v2 @ 2.30 GHz	1
		256 GB RAM	
		Up to 24 internal hard drives	
		Up to 10 Gbps maximum Ethernet port speeds	
	Private IBM Cloud Object Storage endpoint	Closest private domain IBM Cloud Object Storage endpoint (Regional or Cross Regional)	1
	Operating system	Red Hat Enterprise Linux or Ubuntu Linux server	1
Block storage**	1 TB SATA	Operating system and IBM Spectrum Protect instance disk	2 (RAID 1)

	960 GB SSD (3 DWPD)	IBM Spectrum Protect database disk	8 (RAID 5)***
	8 TB SATA	IBM Spectrum Protect database backup disk	3 (RAID 5)
	960 GB SSD (3 DWPD)	IBM Spectrum Protect database active log disk	1
	1 TB SATA	IBM Spectrum Protect database archive log disk	5 (RAID 5)
	960 GB SSD (3 DWPD)	IBM Spectrum Protect cloud cache disk	5 (RAID 5)
Object storage	IBM Cloud Object Storage, Standard Storage Class, Regional or Cross Regional Bucket	IBM Spectrum Protect bucket Closest endpoint to server Accessed via private IBM Cloud endpoint using HTTPS	1

** This configuration uses 96 hyperthreaded Intel cores.*

*** This configuration provides no hot spare coverage. A maximum of 24 in-chassis drive slots are used.*

**** Consider combining the database and the active log in the same array for greater database capacity.*

Table 4: IBM Cloud, large configuration, disk-to-cloud tiering

Cloud component	**IBM Cloud component**	**Detailed description**	**Quantity**
Server and network	Intel Xeon E5-2690 v4 (bare metal server)	28-core* Intel Xeon CPU E5-2690 v4 @ 2.60 GHz	1
		256 GB RAM	

		Up to 36 internal hard drives Up to 10 Gbps maximum Ethernet port speeds	
	Private IBM Cloud Object Storage endpoint	Closest private domain IBM Cloud Object Storage endpoint (Regional or Cross Regional)	1
	Operating system	Red Hat Enterprise Linux or Ubuntu Linux server	1
Block storage	1 TB SATA	Operating system and IBM Spectrum Protect instance disk	2 (RAID 1)
	960 GB SSD (3 DWPD)	IBM Spectrum Protect database disk	8 (RAID 5)**
	960 GB SSD (3 DWPD)	IBM Spectrum Protect database active log disk	1
	8 TB SATA	IBM Spectrum Protect database backup, database archive log, and disk container pool tier disk	12 (RAID 6) 12 (RAID 6) 1 hot spare
Object storage	IBM Cloud Object Storage, Standard Storage Class, Regional or Cross Regional Bucket	IBM Spectrum Protect bucket Closest endpoint to server	1

		Accessed via private IBM Cloud endpoint using HTTPS	

** This configuration uses 56 hyperthreaded Intel cores.*

*** Consider combining the database and the active log in the same array for greater database capacity.*

Table 5: IBM Cloud, medium configuration, direct-to-cloud model

Cloud component	**IBM Cloud component**	**Detailed description**	**Quantity**
Server and network	Intel Xeon E5-2650 v4 (bare metal server)	24-core* Intel Xeon CPU E5-2650 v4 @ 2.20 GHz	1
		128 GB RAM	
		Up to 36 internal hard drives	
		Up to 10 Gbps maximum Ethernet port speeds	
	Private IBM Cloud Object Storage endpoint	Closest private domain IBM Cloud Object Storage endpoint (Regional or Cross Regional)	1
	Operating system	Red Hat Enterprise Linux or Ubuntu Linux server	1
Block storage**	1 TB SATA	Operating system and IBM Spectrum Protect instance disk	2 (RAID 1)
	960 GB SSD (3 DWPD)	IBM Spectrum Protect database disk	5 (RAID 5) 1 hot spare

	4 TB SATA	IBM Spectrum Protect database backup disk	3 (RAID 5) 1 hot spare
	960 GB SSD (3 DWPD)	IBM Spectrum Protect database active log disk	1
	1 TB SATA	IBM Spectrum Protect database archive log disk	4 (RAID 5) 1 hot spare
	960 GB SSD (3 DWPD)	IBM Spectrum Protect cloud cache disk	3 (RAID 5) 1 hot spare
Object storage	IBM Cloud Object Storage Standard Regional Vault	IBM Spectrum Protect vault Same IBM Cloud Region as server Accessed via private IBM Cloud endpoint using HTTPS	1

** This configuration uses 48 hyperthreaded Intel cores.*

*** The server chassis has available drive slots that can be used to increase the number of drives in the database backup array to increase database backup capacity (number of days).*

Table 6: IBM Cloud, medium configuration, disk-to-cloud tiering

Cloud component	IBM Cloud component	Detailed description	Quantity
Server and network	Intel Xeon E5-2650 v4 (bare metal server)	24-core* Intel Xeon CPU E5-2650 v4 @ 2.20 GHz	1
		128 GB RAM	

		Up to 36 internal hard drives	
		Up to 10 Gbps maximum Ethernet port speeds	
	Private IBM Cloud Object Storage endpoint	Closest private domain IBM Cloud Object Storage endpoint (Regional or Cross Regional)	1
	Operating system	Red Hat Enterprise Linux or Ubuntu Linux server	1
Block storage**	1 TB SATA	Operating system and IBM Spectrum Protect instance disk	2 (RAID1)
	960 GB SSD (3 DWPD)	IBM Spectrum Protect database disk	5 (RAID 5) 1 hot spare
	960 GB SSD (3 DWPD)	IBM Spectrum Protect database active log disk	1
	8 TB SATA	IBM Spectrum Protect database backup, database archive log, and disk container pool tier	16 (RAID 6) 1 hot spare
Object storage	IBM Cloud Object Storage, Standard Storage Class, Regional, or Cross Regional Bucket	IBM Spectrum Protect bucket Closest endpoint to server Accessed via private IBM Cloud endpoint using HTTPS	1

** This configuration has 56 hyperthreaded Intel cores.*

*** The server chassis has available drive slots that can be used to increase the number of drives in the shared storage array to increase database backup capacity (number of days). Alternatively, you can create a dedicated database backup array for this storage purpose.*

Table 7: IBM Cloud, small configuration, direct-to-cloud model

Cloud component	IBM Cloud component	Detailed description	Quantity
Server and network	Intel Xeon E5-2620 v4 (bare metal server)	16-core* Intel Xeon CPU E5-2620 @ 2.10 GHz	1
		64 GB RAM	
		Up to 36 internal hard drives	
		Up to 10 Gbps maximum Ethernet port speeds	
	Private IBM Cloud Object Storage endpoint	Closest private domain IBM Cloud Object Storage endpoint (Regional or Cross Regional)	1
	Operating system	Red Hat Enterprise Linux or Ubuntu Linux server	1
Block storage**	1 TB SATA	Operating system and IBM Spectrum Protect instance disk	2 (RAID 1)
	960 GB SSD (3 DWPD)	IBM Spectrum Protect database disk	3 (RAID 5) 1 hot spare

	2 TB SATA	IBM Spectrum Protect database backup disk	3 (RAID 5) 1 hot spare
	960 GB SSD (3 DWPD)	IBM Spectrum Protect database active log disk	1
	1 TB SATA	IBM Spectrum Protect database archive log disk	2 (RAID 1) 1 hot spare
	960 GB SSD (3 DWPD)	IBM Spectrum Protect cloud cache disk	3 (RAID 5) 1 hot spare
Object storage	IBM Cloud Object Storage Standard Regional Vault	IBM Spectrum Protect vault (same IBM Cloud Region as server) Accessed via private IBM Cloud endpoint using HTTPS	1

** This configuration has 32 hyperthreaded Intel cores.*

*** The server chassis has available drive slots that can be used to increase the number of drives in the database backup array to increase database backup capacity (number of days).*

Table 8: IBM Cloud, small configuration, disk-to-cloud tiering

Cloud component	IBM Cloud component	Detailed description	Quantity
Server and network	Intel Xeon E5-2620 v4 (bare metal server)	16-core* Intel Xeon CPU E5-2620 @ 2.10 GHz	1
		64 GB RAM	
		Up to 36 internal hard drives	

		Up to 10 Gbps maximum Ethernet port speeds	
	Private IBM Cloud Object Storage endpoint	Closest private domain IBM Cloud Object Storage endpoint (Regional or Cross Regional)	1
	Operating system	Red Hat Enterprise Linux or Ubuntu Linux server	1
Block storage**	1 TB SATA	Operating system and IBM Spectrum Protect instance disk	2 (RAID 1)
	960 GB SSD (3 DWPD)	IBM Spectrum Protect database disk	3 (RAID 5) 1 hot spare
	960 GB SSD (3 DWPD)	IBM Spectrum Protect database active log disk	1
	8 TB SATA	IBM Spectrum Protect database backup, database archive log, and disk container pool tier disk	8 (RAID 6) 1 hot spare
Object storage	IBM Cloud Object Storage, Standard Storage Class, Regional, or Cross Regional Bucket	IBM Spectrum Protect bucket Closest endpoint to server Accessed via private IBM Cloud endpoint using HTTPS	1

** This configuration has 32 hyperthreaded Intel cores.*

*** The server chassis has available drive slots that can be used to increase the number of drives in the shared storage array to increase database backup capacity (number of days). Alternatively, you can create a dedicated database backup array for this storage purpose.*

Table 9: IBM Cloud, extra-small configuration, direct-to-cloud model

Cloud component	**IBM Cloud component**	**Detailed description**	**Quantity**
Server and network	M1.4x32 IBM Cloud virtual server	4-core Intel Xeon CPU E5-2683 @ 2.10 GHz	1
		32 GB RAM	
		Portable SAN storage volumes (PSVs)	
		Up to 1 Gbps maximum Ethernet port speeds	
	Private IBM Cloud Object Storage endpoint	Closest private domain IBM Cloud Object Storage endpoint (Regional or Cross Regional)	1
	Operating system	Red Hat Enterprise Linux or Ubuntu Linux server	1
Block storage	100 GB SAN-attached PSV	Operating system and IBM Spectrum Protect instance disk	1
	300 GB SAN-attached PSV	IBM Spectrum Protect database and active log disk	1 (divided into five file systems using LVM)
	500 GB SAN-attached PSV	IBM Spectrum Protect database backup and archive log disk	1 (divided into separate file systems using LVM)

	1 TB SAN-attached PSV	IBM Spectrum Protect cloud cache disk	1
Object storage	IBM Cloud Object Storage Standard Regional Vault	IBM Spectrum Protect vault (same IBM Cloud region as server) Accessed via private IBM Cloud endpoint using HTTPS	1

2.1 Design Considerations for IBM Cloud Systems

A plethora of **bare metal server and virtual server** options are available with IBM Cloud that might be suitable for use with IBM Spectrum Protect. Key aspects to keep in mind with IBM Cloud are the possible need to purchase additional **public bandwidth** if the server is used for backup operations from external clients outside of the IBM Cloud network or to secure a dedicated **network line** from a primary server site if the cloud-based server is being used as a replication target in a DR scenario (via the IBM Cloud Direct Link service). The best option will depend on network requirements and the anticipated amount of data being moved by replication or storage pool protection per day. Select **10 Gbps public and private network uplinks** for the large, medium, and small bare metal server options to help ensure sufficient backup network and object storage network capacity for the system. Select 1 Gbps public and private network uplinks for the extra-small virtual server option.

Select an IBM Cloud bare metal server that can manage enough **internal disks** for the planned large, medium, or small deployment. Some systems feature as few as 4 or as many as 36 internal disks as an option. The number of required disks can quickly increase when factoring in RAID requirements. If the drive chassis has open, unused drive slots, consider adding drives for array hot spare coverage as an added precaution. Disk outages can occur with IBM Cloud bare metal servers, and you must open a device-oriented service ticket with the IBM Cloud support team to resolve them. Another possible use for additional drive slots within the chassis is to increase capacity for storage of additional Db2 database backup generations. If needed, consider combining the IBM Spectrum Protect **database and active log disks** into a single RAID 5 array to conserve disk count and increase database capacity.

SSD disks are preferable for the underlying IBM Spectrum Protect database, database active log, and cloud accelerator cache. Higher-capacity SATA drives are a suitable IBM Cloud hosted option for underlying the database backup volumes, database archive log, and directory-container storage pool disk tier when grouped together with RAID protection and possible hot spare coverage. To correct a disk outage with IBM Cloud, you must open a service ticket with the hardware support team. RAID protection for storage pool, database archive log, and database backup disks is preferred, with hot spares utilized if in-chassis drive capacity is present.

2.1.1 Considerations for Direct-to-Cloud Architectures

The **direct-to-cloud** configurations discussed previously are architected such that the disk of the cloud accelerator cache is on fast-performing SSD. In general, the limiting factor for end-to-end ingestion throughput for an IBM Spectrum Protect server using object storage is the network to the object storage system or the object storage system itself. For this reason, you must understand the throughput capability requirements of the planned system. Those requirements will drive your decisions about assigning servers to Ethernet networks. Next, the ceiling for daily ingestion throughput (in terms of mebibytes per second or tebibytes per day) must be understood at the object storage end via **object storage benchmarking** tests. The test results will establish what the overlapped I/O capability would have to be for the cloud accelerator cache disk location for maximum back-end throughput. These two factors will help you select a disk technology to sustain daily backup ingestion needs while working within object storage limits. After you select a disk technology, run **disk benchmarking** tests to ensure throughput capability (see Disk Benchmarking).

Tip: In this paper, the abbreviation MiB is used for mebibytes, the abbreviation TiB is used for tebibytes, the abbreviation KiB is used for kibibytes, and the abbreviation GiB is used for gibibytes.

Example

If an object storage link is capable of 10 Gbps, this equals about 1000 MiB/s after packet overhead and other efficiency loss. In order to saturate this link for long periods, the cloud accelerator cache disk location must be capable of taking in client ingestion data (writes) at 1000 MiB/s and transmitting staged data to object storage (reads) at a similar 1000 MiB/s (~128-256 KiB I/O size). This capacity ensures that the cloud accelerator cache disk can remain as small as possible while sustaining maximum throughput. **Alternatively**, a larger capacity, slower disk technology (such as SATA) can be used such that the client ingestion data that has been staged to accelerator disk cache can be transmitted to object storage over a longer period of the day (extending past the backup window). However, beware that data residing only in the cloud accelerator cache is unprotected in the sense that only a single copy of the data exists. The redundancy protection inherent in cloud object storage is available only if the data is transmitted to object storage. The disk used for the cloud accelerator cache should be protected by RAID (in the case of physical disks) to avoid data loss, and the disk should be performant enough to allow quick data transfer to object storage. Generally, IBM Cloud virtual server portable SAN storage volumes (PSVs) provide acceptable durability.

2.1.2 Sizing the Cloud Accelerator Cache

Figure 4 can be used as a rough guide for the appropriate disk technology to use based on object storage and object storage network capability. At the top left, IBM Cloud Object Storage is reachable over the same LAN (for example, with an IBM Cloud bare metal server over the private IBM Cloud network). As we move from top to bottom in the diagram, the network capability becomes slower (10 Gbps to 1 Gbps), while the storage capacity needs increase to store data that is queued up in the accelerator disk cache awaiting transfer to object storage. In the case of slower network-to-object storage, it is more likely that (asynchronous) client ingestion from local client systems can run at a faster rate than cloud transfer. In such a scenario, client ingestion data begins to fill the cache disk location faster than the data can be transferred to object storage and cleared from the cache. As of IBM Spectrum Protect V8.1.2, an internal **throttling** mechanism is in place to slow client ingestion speeds if the cloud accelerator cache disk area begins nearing capacity. However, to avoid slowing client ingestion in cases where ingestion exceeds the cloud transfer rate (which might not be desired), the accelerator cache should be sized with a larger capacity, perhaps up to a single day's worth of back-end client ingestion (after data deduplication and compression).

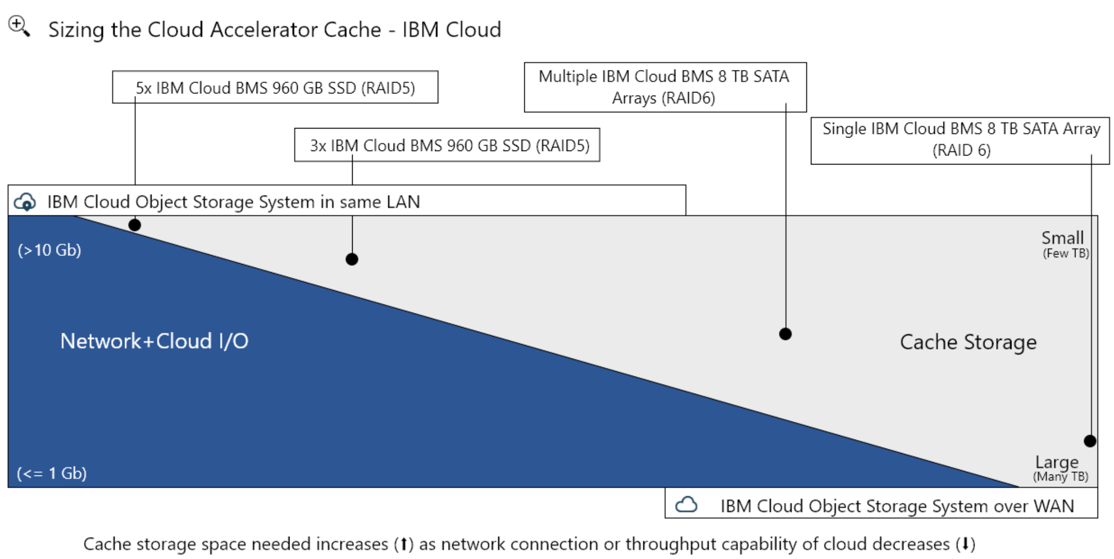


Figure 4: Sizing the cloud accelerator cache for IBM Cloud

2.1.3 Considerations for Disk-to-Cloud Tiering Architectures

When using the **disk-to-cloud tiering** model, it is important to **adequately size** the directory-container storage pool disk tier to be large enough to hold operational recovery data and provide a buffer to avoid backup or archive failures. An understanding of the tiering storage rules to be used and the effect on the quantity of data that will remain in the disk tier should be established

For data that **does not deduplicate well** (highly unique data that changes between backup operations), each backup generation will be mostly unique compared to the previous. This scenario allows for a good estimation of what the daily ingestion and tier quantities will be. For example, if you want to maintain 5 days' worth of operational recovery data on the disk tier, a storage rule with a `TIERDELAY` value of 5 would result in backup generations 6 days or older being tiered to object storage when the tiering storage rule process runs. The directory-container storage pool should be sized large enough to hold at least 6 days' worth of backup data (5 days for operational recovery and 1 for the "buffer" of ingesting a new day's worth of data). Additional days of sizing will help protect against accidental overruns to the disk tier. This can happen, for example, in case of an interruption or loss of service to the object storage endpoint underlying the cloud-container storage pool involved in tiering or if a larger quantity of backup ingestion is experienced on a given day (such as when new systems are backed up for the first time). Unlike the direct-to-cloud path with cloud accelerator cache, there is no throttling mechanism in place to slow client ingestion to a near-full directory-container storage pool. Backup failures could result if the disk tier runs out of capacity.

Beware that the **`REUSEDELAY`** setting for the directory-container storage pool serving as the disk tier can influence how much data is preserved in this disk tier. This storage pool parameter controls how many days' worth of deduplicated extents are kept in the storage pool after their reference count has reached zero. A value of 0 will cause deduplicated extents to be removed from the disk tier soon after their reference counts have reached zero (for example, after objects with very little data overlap and low data deduplication are tiered to object storage). A value of 1 or more days can be used to preserve deduplicated extents in the directory-container storage pool such that new client ingestion is more likely to match these extents. This situation could lower IOPs and throughput demands to the disk tier because these data extents will not need to be rewritten. If client-side data deduplication is used, this feature can also decrease network demands for these clients. However, increasing the value of the `REUSEDELAY` parameter on the directory-container storage pool disk tier might increase capacity demands to the disk tier because more data is preserved.

IBM Cloud Block Storage should generally be **avoided** for use as directory-container storage pool disk tier storage. Instead, use internal drive chassis disks within the bare metal server. The most affordable endurance storage cost with IBM Cloud Block Storage is $0.10 per GiB monthly. The large disk-to-cloud tiering configuration outlined in this paper involves a disk tier with 140 TiB of raw capacity after accounting for 16 TiB for database backup and 4 TiB for Db2 archive log from the initial 160 TB raw capacity provided by the two 12-drive 8 TiB RAID6 SATA disk arrays. The cost for 140 TiB of IBM Cloud Block storage at the cheapest endurance level would be $14,336 monthly. In-chassis disk arrays with bare metal servers provide for the most cost-effective block storage option with IBM Cloud.

The following table illustrates how the disk-to-cloud tiering configurations outlined in this paper could be adjusted to feature greater capacity in the operational recovery disk tier or greater capacity for the IBM Spectrum Protect database. In general, consider using larger capacity SATA drives (such as 10 or 12 TB) for disk tier arrays or larger capacity SSD drives (such as 1.7 TB SSD 3 DWPD or 3.8 TB SSD 3 DWPD) for the database array, or both. Alternatively, if drive slots are available in the server chassis, consider adding additional drives to the RAID groups to increase capacity.

Goal	Small configuration	Medium configuration	Large configuration
Original	Database array: 3x 960 GB SSD (RAID 5) + hot spare Disk tier array: 8x 8 TB SATA (RAID 6) + hot spare	Database array: 5x 960 GB SSD (RAID 5) + hot spare Disk tier array: 16x 8 TB (RAID 6) + hot spare	Database array: 8x 960 GB SSD (RAID 5) Disk tier array: 12x 8 TB (RAID 6) + 12x 8 TB (RAID 6) + hot spare
Greater disk tier capacity	Disk tier array: 8x 12 TB SATA (RAID 6) + hot spare ***(+24 TB raw)***	Disk tier array: 16x 12 TB (RAID 6) + hot spare ***(+56 TB raw)***	Disk tier array: 12x 12 TB (RAID 6) + 12x 12 TB (RAID 6) + hot spare ***(+80 TB raw)***
Greater database capacity	Database array: 3x 1.7 TB SSD (RAID 5) + hot spare ***(+1.5 TB raw)***	Database array: 4x 1.7 TB SSD (RAID 5) + hot spare ***(+1.35 TB raw)***	Database array: 7x 1.7 TB SSD (RAID 5) ***(+3.6 TB raw)***

The **storage rule** for disk-to-cloud tiering can be defined with a `MAXPROCESS` parameter value in the range 1 - 99. For optimal throughput, the following values are preferred based on the disk-to-cloud tiering configuration size outlined in this paper:

- **Small: 10 processes**
- **Medium: 25 processes**
- **Large: 35 - 50 processes**

In practice, the performance of disk-to-cloud tiering might not be a critical concern. In this case, lower `MAXPROCESS` values can be used to transfer tiered data over a longer duration of time outside of the backup window.

2.1.4 Disk-to-Cloud Tiering Operational Recovery Capacities

The disk-to-cloud tiering architectures presented in this paper are configured with shared, in-chassis RAID 6 SATA disk arrays that field the responsibility for the directory-container storage pool disk tier, Db2 database backup, and the Db2 archive log. For Linux systems, LVM can be used to create multiple logical volumes from a single physical disk presented to the operating system. For the configurations presented in this paper, LVM was used to establish volumes in the following manner:

Small

- 8-disk 8 TiB RAID 6 Array (48 TiB raw capacity)
    - 1 physical volume and volume group
        - 2 logical volumes, 2 TB each for database backup
        - 1 logical volume, 1 TB for archive log
        - 1 logical volume, 43 TB for disk tier

Medium

- 16-disk 8 TiB RAID 6 Array (112 TiB raw capacity)
    - 1 physical volume and volume group
        - 2 logical volumes, 4 TB each for database backup
        - 1 logical volume, 3 TB for archive log
        - 1 logical volume, 101 TB for disk tier

Large

- 12-disk 8 TiB RAID 6 Array (80 TiB raw capacity) (first)
    - 1 physical volume and volume group
        - 1 logical volume, 8 TB for database backup
        - 1 logical volume, 4 TB for archive log
        - 1 logical volume, 68 TB for disk tier
- 12-disk 8 TiB RAID 6 array (80 TiB raw capacity) (second)
    - 1 physical volume and volume group
        - 1 logical volume, 8 TB for database backup
        - 1 logical volume, 72 TB for disk tier

Each of the disk tier logical volumes for each configuration was then formatted as an **XFS file system**. This approach yielded the following usable capacities for an operational recovery disk tier.

Table 10: Operational recovery data with disk-to-cloud tiering

Sizing category	Daily ingestion data (front-end)	Disk tier usable capacity	Days of operational recovery data on disk*
Small	Up to 10 TB per day	38.66 TB	About 3 or more
Medium	10 – 20 TB per day	90.87 TB	About 5 or more
Large	20 – 100 TB per day	125.53 TB	About 5 or more

** The estimate is based on a workload with a high daily change rate and minimal data deduplication.*

A **1-day buffer** is factored in to account for newly ingested data entering the disk tier during a backup window before the next daily tiering operation can run. Estimates for the number of days of operational recovery data presented in the table reflect an assumption that the ingested workload is mostly unique from day to day (minimal data deduplication). The lower end of daily ingestion ranges accounts for scenarios in which ingested data does not deduplicate or compress well, or both. The lower end of the ranges for small, medium, and large were used to estimate the number of (age-based tiering) days of operational recovery data that can be preserved on the directory-container storage pool disk tier.

The value of the **`REUSEDELAY`** parameter for the directory-container storage pool disk tier must also be considered when sizing disk tier capacity, as an increase in this value above 0 can cause additional data to be preserved in the directory-container storage pool.

2.1.5 IBM Cloud Object Storage Resiliency and Storage-Class Choices

Cloud object storage provided by IBM Cloud, using the Simple Storage Server (S3) protocol, is available in three **Resiliency** choices:

- With Cross Region resiliency, data is stored across three regions within a geography for regional concurrent access and highest availability.
- With Regional resiliency, data is stored in multiple data center facilities within a single geographic region for high availability.
- With Single Data Center resiliency, data is stored across multiple devices in a single data center for data locality and local access (see References [4]).

Cross Region resiliency is more expensive from a capacity standpoint than Regional and Single Data Center. As of this writing, Single Data Center is available in a small number of locations. Regional object storage endpoints exist in US South and East locations as well as in Great Britain, Germany, and Japan. Cross-regional endpoints exist across US, European, and Asia-Pacific locations. Endpoints are frequently being added. Visit the IBM Cloud website for the most current listing of object storage options.

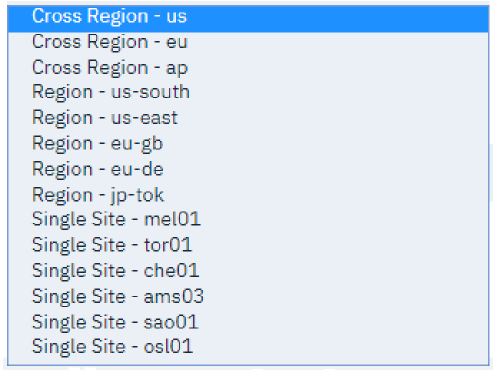


Figure 5: Cross-regional endpoints

IBM Cloud Object Storage buckets with any of these Resiliency choices can be used with an IBM Spectrum Protect cloud-container storage pool. When selecting an IBM Cloud Object Storage endpoint, be sure to select the private network endpoint that is closest to the IBM Cloud bare metal server that is being used in order to minimize latency and achieve the best throughput performance. Throughput to an object storage endpoint should be benchmarked to determine what level of throughput is possible from a bare metal server to that endpoint (see Object Storage Benchmarking). Bandwidth and latency can vary by data center. For the environments configured in the test lab for this paper, the Dallas 05 data center was chosen for IBM Cloud bare metal server resources. The US South (Regional) and the Dallas Cross Regional endpoints were compared with similar ingestion throughput achieved to each (see Throughput Measurements and Results). However, individual deployment results can vary. IBM Spectrum Protect currently does not alter behavior based on the Resiliency of a bucket.

IBM Cloud Object Storage is furthermore offered in three **Storage-class** choices: Standard, Vault, and Cold Vault, where capacity costs are lower in the case of Vault and Cold Vault, but with higher HTTP GET costs associated with data recovery. For use with IBM Spectrum Protect, generally the **Standard** storage class should be used for most backup data. For long-term retention and archive data which is rarely restored, Vault or Cold Vault could be considered to save on capacity costs. Cold Vault can be used in a disk-to-cloud tiering architecture where data demoted to object storage is older, inactive, or both and is unlikely to be restored often.

2.1.6 An Alternative Large Disk-to-Cloud Tiering Architecture

At publication time, a monthly-provisioned IBM Cloud bare metal server option featuring both quad-socket processors and greater than 24 internal drive chassis slots did not exist. As such, the large disk-to-cloud tiering configuration outlined in this paper differs in the bare metal server model from the large direct-to-cloud model. A tradeoff was made between CPU capacity and in-chassis drive capacity. In practice, the large direct-to-cloud variation (quad-socket, Intel Xeon E7-4890 v2 processors) proved capable of exceeding preexisting daily ingest targets for cloud-container storage pools (see Throughput Measurements and Results). The two additional processor sockets and CPU threads enabled more efficient IBM Spectrum Protect data deduplication and compression processing. The disk-to-cloud tiering server model (Intel Xeon E5-2690) features two processor sockets and fewer CPU threads and was capable of sustaining data movement to object storage via tiering to satisfy large Blueprint performance targets.

For greater daily ingestion throughput capability to object storage, consider the following alternative: a large disk-to-cloud tiering configuration. This configuration features the same bare metal server model as the direct-to-cloud configuration (to take advantage of the additional processor sockets and CPU threads), but with larger disk capacities to allow for operational recovery data to fit within only 24 available drive chassis slots. This solution involves combining the roles of the database disk and active log disk into a single 6-disk RAID 5 array. In this case, LVM or another software-based volume utility should be used to create at least 8 separate database volumes and 1 active log volume from this array for use by IBM Spectrum Protect. 12 TiB drives are used instead of 8 TiB drives for the two RAID 6 arrays responsible for the disk tier, database backup, and archive log. Note that no hot spare is provisioned in this case. However, RAID 6 protection does ensure that up to 2 disks can be lost in each array.

With the same allocations of 16 TiB for database backup and 4 TiB for archive log usage, the following configuration results in approximately 124 TiB of raw capacity for use by a disk tier. This should equate to approximately 110 TiB of usable file system capacity, allowing for approximately 4 or more days of operational recovery data preserved on the disk tier.

Table 11: IBM Cloud, large alternative configuration, disk-to-cloud tiering

Cloud component	**IBM Cloud component**	**Detailed description**	**Quantity**
Server and network	Intel Xeon E7-4850 v2 (bare metal server)	48-core* Intel Xeon CPU E7-4850 v2 @ 2.30 GHz	1
		256 GB RAM	
		Up to 24 internal hard drives	
		Up to 10 Gbps maximum Ethernet port speeds	
	Private IBM Cloud Object Storage endpoint	Closest private domain IBM Cloud Object Storage endpoint (Regional or Cross Regional)	1

	Operating system	Red Hat Enterprise Linux or Ubuntu Linux server	1
Block storage	1 TB SATA	Operating system and IBM Spectrum Protect instance disk	2 (RAID 1)
	1.7 TB SSD (3 DWPD)	IBM Spectrum Protect database and active log disk	6 (RAID 5)
	12 TB SATA	IBM Spectrum Protect database backup, database archive log, and disk container pool tier disk	8 (RAID 6) 8 (RAID 6)
Object storage	IBM Cloud Object Storage, Standard Storage Class, Regional, or Cross Regional Bucket	IBM Spectrum Protect bucket Closest endpoint to server Accessed via private IBM Cloud endpoint using HTTPS	1

** This configuration uses 56 hyperthreaded Intel cores.*

Throughput Measurements and Results

Throughput measurements for backup and restore operations are provided with representative data sets for selected configurations. Throughput measurements are included for IBM Spectrum Protect configurations involving a direct-to-cloud model with cloud accelerator cache and for configurations involving disk-to-cloud tiering.

For each configuration tested, the following preferred settings were adopted for the cloud-container storage pool. To optimize performance when you deploy an IBM Spectrum Protect server instance in the cloud, use the following settings:

- Storage pool compression enabled
- Storage pool encryption enabled
- Storage pool configured as an off-premises cloud-container storage pool

- HTTPS URLs specified for all cloud endpoints

3.1 Data Set Descriptions

For the performance tests that were conducted within these environments, all or a subset of the following data sets were used:

Table 12: Throughput measurement data sets

Front-end object size	Average duplication extent size	Duplicate data percentage	Data compressibility	Notes
128 MiB	~150-200 KiB	~70%	~50%	VE-like, favorable extent size
128 MiB	~200-300 KiB	~0%	~0%	Random data, large extent size
1 GiB	~60-100 KiB	~50%	~50%	DB-like, small extent size

The **128 MiB, VE-like** front-end data set represents a relatively large object size that aligns with the IBM Spectrum Protect for Virtual Environments: Data Protection for VMware API client's **VE megablock** size for virtual machine disk backups. The large object size and **relatively large, though realistic, deduplication extent** size represents a favorable profile for the IBM Spectrum Protect server's ingestion engine to achieve good performance. A duplicate data rate of 70% combined with a compressibility rate of 50% for this data set yields an **85% total data reduction** from front-end data as compared with data that is actually stored to the (cloud-accelerator cache and object storage) back end after data deduplication, compression, and encryption processing. Although this workload does not qualify as a "best case," it does represent a realistic, favorable scenario in which to model top-end throughput capability of an IBM Spectrum Protect system without overestimating throughput performance.

The **128 MiB, random** front-end data set represents a larger object size with a large, favorable deduplication extent size. However, the random nature of the data ensures that it does not deduplicate well with existing storage pool data or compress well. This data set is included to represent a workload that is throughput intensive from the perspective of storage pool disk and object storage network load. Full backups of large objects containing relatively random data content would be modeled well by this data set.

The **1 GiB** front-end data set represents a model of **structured, database-like data** possessing a relatively small deduplication extent size relative to the front-end object size.

Such a workload is representative of what might be experienced with an IBM Spectrum Protect for Databases: Data Protection for Oracle backup environment protecting production databases. The smaller extent size causes additional strain and overhead for the IBM Spectrum Protect ingestion engine and typically results in less throughput than the 128 MiB data set. A duplicate data rate of 50% and compressibility of 50% yield a 75% overall front-end to back-end reduction for this workload, with a **4:1 ratio** reduction, which approaches what is seen for this type of data in the field.

3.2 Backup and Restore Measurements

The following sections outline the backup and restore throughput results that were experienced in the IBM Cloud environments that were built. Each IBM Cloud bare metal server was deployed in the **Dallas 05 IBM Cloud** data center. Throughput measurements were conducted and are presented here **both for IBM Cloud Regional and Cross Regional** Cloud Object Storage targets. The following closest endpoints were used for object storage testing:

- **IBM Cloud Regional (South):**
    - https://s3.us-south.objectstorage.service.networklayer.com
- **IBM Cloud Cross Regional (Dallas endpoint):**
    - https://s3-api.dal-us-geo.objectstorage.service.networklayer.com

Prior to conducting backup and restore tests on the IBM Spectrum Protect environments, a **load phase** was conducted whereby the servers were initially loaded with a set of deduplicated 128 MiB front-end data to populate the server database tables and provide for a more realistic customer configuration. IBM Spectrum Protect database queries can change their behavior based on the size and layout of server database tables. This load phase was necessary to bring behavior in line with real environment expectations.

For each data set, up to 50 IBM Spectrum Protect client backup sessions were initiated in parallel to the large server, up to 25 for the medium server, up to 10 for the small server, and up to 5 for the extra-small server. The results presented here for backup represent the maximum front-end throughput experienced with the largest number of sessions tested against that system.

For each data set that was restored, between 1 and 20 client restore sessions were initiated for the large and medium systems and between 1 and 10 for the small system. Results presented here include the intermediate session count values to give an idea on how restore throughput can scale with the number of restore sessions involved for data sets similar to these types.

All throughput values represent front-end, "protected data" values, before inline data deduplication, compression, and encryption. These are the data rates experienced by a **client** that is backing up data to or restoring data from the IBM Spectrum Protect server. The rates are similar to what customers would likely describe as their performance experience with the product. On ingestion, the actual quantity of data that makes it to accelerator cache disk and onwards to object storage will be less, depending on the data deduplication and compression rate. On restore, all individual extents comprising a front-end object will be restored using HTTP GET calls from the object storage device if those objects are resident in the cloud-container storage pool. However, the built-in caching within the IBM Spectrum Protect server's restore engine might reduce the number of restore operations that are required if a workload contains duplicate data.

Restore throughput results are provided for the **disk-to-cloud tiering** architectures from the directory-container storage pool disk tier as a reference for restore capability from the operational recovery tier.

3.2.1 IBM Cloud: Large Instance Measurements for the Direct-to-Cloud Model

128 MiB VE-like front-end data set results (at 50 front-end sessions):

Table 13: IBM Cloud, large configuration, direct-to-cloud model, 128 MiB VE-like data set backup results

IBM Cloud Object Storage	Data deduplication %	MiB/s	TiB/hour	TiB per 8 hours	TiB per 10 hours
Cross Regional	70%	3504.9	12.0	96.2	120.3
Regional	70%	3462.1	11.9	95.1	118.9

For the large IBM Cloud build, front-end aggregate throughput for the 50-session favorable data set achieved 12.0 TiB/hour, which would yield capability well within the large Blueprint range. Values are provided here for estimates using both 8-hour and 10-hour backup windows on a given day. Both estimates are provided for convenience to align with our experience that customers generally use one of these two time periods for their daily ingestion workloads.

Table 14: IBM Cloud, large configuration, direct-to-cloud model, 128 MiB VE-like data set restore

Sessions	Cross Regional MiB/s	Cross Regional GiB/hour	Regional MiB/s	Regional GiB/hour

1	133.4	468.9	189.7	667.1
2	279.4	982.1	379.1	1332.9
4	588.5	2069.1	765.9	2692.6
5	728.5	2561.2	963.5	3387.4
8	1167.2	4103.5	1533.2	5390.1
10	**1291.8**	**4541.6**	**1776.8**	**6246.6**
15	782.1	2749.7	1392.2	4894.4
16	865.3	3041.9	1461.1	5136.6
20	824.6	2899.1	1299.0	4566.9

Restore rates from object storage are typically challenged due to latency and individual read characteristics. Restore throughput rates with realistic session counts from object storage pools might challenge certain data recovery time objectives (RTOs). Overall, with this configuration and data set, throughput of approximately 50 MiB/s per session for up to 10 sessions can be expected. Thereafter, you can expect diminishing returns regarding throughput.

128 MiB random front-end data set results:

Table 15: IBM Cloud, large configuration, direct-to-cloud model, 128 MiB random data set backup results

IBM Cloud Object Storage	Data deduplication %	MiB/s	TiB/hour	TiB per 8 hours	TiB per 10 hours
Cross Regional	0%	362.2	1.24	9.9	12.4
Regional	0%	508.0	1.74	13.9	17.4

For the large IBM Cloud build, front-end aggregate throughput for the 50-session random data set with minimal data deduplication and compression achieved 1.2-1.7 TiB/hour. This is a poor scenario that is likely to be unrealistic in practice.

Table 16: IBM Cloud, large configuration, direct-to-cloud model, 128 MiB random data set restore

Sessions	Cross Regional MiB/s	Cross Regional GiB/hour	Regional MiB/s	Regional GiB/hour
1	94.5	332.2	133.8	470.4
2	170.4	599.0	225.1	791.3
4	225.7	793.4	351.3	1235.2
5	243.5	856.1	387.3	1361.5
8	266.5	936.9	294.8	1036.4
10	265.9	934.8	307.9	1082.5
15	296.0	1040.6	355.8	1250.9
16	300.3	1055.9	387.7	1363.1
20	263.4	926.1	398.5	1400.8

1 GiB front-end data set results:

Table 17: IBM Cloud, large configuration, direct-to-cloud model, 1 GiB data set backup results

IBM Cloud Object Storage	Data deduplication %	MiB/s	TiB/hour	TiB per 8 hours	TiB per 10 hours
Cross Regional	50%	1910.4	6.56	52.5	65.6
Regional	50%	2260.6	7.76	62.1	77.6

Ingestion throughput rates with the 1 GiB data set featuring the smaller (60 – 100 KiB) average deduplication extent size were less than the 128 MiB favorable workload, but still in line with large Blueprint throughput targets in this direct-to-cloud configuration.

Table 18: IBM Cloud, large configuration, direct-to-cloud model, 1 GiB data set restore results

Sessions	Cross Regional MiB/s	Cross Regional GiB/hour	Regional MiB/s	Regional GiB/hour
1	73.5	258.4	135.5	476.4
2	132.7	466.3	286.8	1008.2
4	258.4	908.6	585.6	2058.6
5	333.2	1171.4	723.9	2544.8
8	533.8	1876.7	1211.7	4259.7
10	329.3	1157.6	911.5	3204.5
15	188.3	661.8	492.8	1732.7
16	192.1	675.3	479.4	1685.4
20	193.8	681.2	472.6	1661.4

Restore throughput rates with the smaller extent workload are somewhat less than the favorable, 128 MiB data set. This is due to the additional overhead of more HTTP GET requests necessary to restore this data (smaller extents lead to more operations per front-end restored data). A throughput of more than 1 TiB/hour could be achieved with 20-40 restore sessions of this data type.

3.2.2 IBM Cloud: Medium Instance Measurements for the Direct-to-Cloud Model

128 MiB VE-like front-end data set results (at 25 front-end sessions):

Table 19: IBM Cloud, medium configuration, direct-to-cloud model, 128 MiB VE-like data set backup results

IBM Cloud Object Storage	Data deduplication %	MiB/s	TiB/hour	TiB per 8 hours	TiB per 10 hours
Cross Regional	70%	1947.8	6.69	53.52	66.9
Regional	70%	1910.2	6.56	52.5	65.6

Table 20: IBM Cloud, medium configuration, direct-to-cloud model, 128 MiB VE-like data set restore

Sessions	Cross Regional MiB/s	Cross Regional GiB/hour	Regional MiB/s	Regional GiB/hour
1	162.9	572.7	198.4	697.4
5	749.3	2634.4	760.2	2672.6
10	944.9	3321.8	938.1	3298.0
15	1228.5	4318.9	1204.5	4234.6
20	1478.1	5196.3	1458.0	5125.9

128 MiB random front-end data set results:

Table 21: IBM Cloud, medium configuration, direct-to-cloud model, 128 MiB random data set backup results

IBM Cloud Object Storage	Data deduplication %	MiB/s	TiB/hour	TiB per 8 hours	TiB per 10 hours
Cross Regional	0%	354.3	1.22	9.8	12.2
Regional	0%	314.4	1.08	.8.6	10.8

Table 22: IBM Cloud, medium configuration, direct-to-cloud model, 128 MiB random data set restore

Sessions	Cross Regional MiB/s	Cross Regional GiB/hour	Regional MiB/s	Regional GiB/hour
1	96.4	339.1	130.5	458.7

5	746.1	2623.1	750.9	2640.0
10	931.8	3276.0	924.4	3250.0
15	1230.4	4325.7	1253.0	4405.0
20	1528.2	5372.4	1445.0	5079.9

1 GiB front-end data set results:

Table 23: IBM Cloud, medium configuration, direct-to-cloud model, 1 GiB data set backup results

IBM Cloud Object Storage	Data deduplication %	MiB/s	TiB/hour	TiB per 8 hours	TiB per 10 hours
Cross Regional	50%	1593.7	5.47	43.8	54.7
Regional	50%	1484.2	5.10	40.8	51.0

Table 24: IBM Cloud, medium configuration, direct-to-cloud model, 1 GiB data set restore results

Sessions	Cross Regional MiB/s	Cross Regional GiB/hour	Regional MiB/s	Regional GiB/hour
1	74.7	262.6	154.4	542.6
5	357.9	1258.1	364.1	1279.9
10	398.0	1399.3	349.7	1229.4
15	412.5	1450.3	363.7	1278.6
20	449.6	1580.6	435.0	1529.4

3.2.3 IBM Cloud: Small Instance Measurements for the Direct-to-Cloud Model

128 MiB VE-like front-end data set results (at 10 front-end sessions):

Table 25: IBM Cloud, small configuration, direct-to-cloud model, 128 MiB VE-like data set backup results

IBM Cloud Object Storage	Data deduplication %	MiB/s	TiB/hour	TiB per 8 hours	TiB per 10 hours
Cross Regional	70%	1056.8	3.63	29.0	36.3
Regional	70%	1071.9	3.68	29.4	36.8

Table 26: IBM Cloud, small configuration, direct-to-cloud model, 128 MiB VE-like data set restore

Sessions	Cross Regional MiB/s	Cross Regional GiB/hour	Regional MiB/s	Regional GiB/hour
1	135.3	475.6	205.2	721.2
2	291.4	1024.5	420.2	1477.2
3	419.3	1474.2	638.6	2245.0
4	578.0	2032.0	854.9	3005.5
5	731.6	2571.9	1075.2	3780.0
6	898.6	3159.0	1156.2	4064.9
7	1034.3	3636.2	1488.5	5233.0
8	1155.2	4061.2	1690.8	5944.4
9	1301.4	4575.1	1885.1	6627.3
10	1237.0	4348.7	1809.0	6359.8

128 MiB random front-end data set results:

Table 27: IBM Cloud, small configuration, direct-to-cloud model, 128 MiB random data set backup results

IBM Cloud Object Storage	Data deduplication %	MiB/s	TiB/hour	TiB per 8 hours	TiB per 10 hours
Cross Regional	0%	413.6	1.42	11.4	14.2
Regional	0%	369.2	1.27	10.2	12.7

Table 28: IBM Cloud, small configuration, direct-to-cloud model, 128 MiB random data set restore

Sessions	Cross Regional MiB/s	Cross Regional GiB/hour	Regional MiB/s	Regional GiB/hour
1	80.3	282.3	126.9	446.2
2	152.0	534.3	227.9	801.2
3	186.4	655.2	297.5	1046.0
4	211.7	744.4	360.9	1268.7
5	210.5	740.1	347.2	1220.8
6	216.3	760.4	407.5	1432.7
7	230.5	810.3	441.7	1552.7
8	237.3	834.3	233.3	820.1
9	152.6	536.4	234.1	823.2
10	173.4	609.5	462.6	1626.4

1 GiB front-end data set results:

Table 29: IBM Cloud, small configuration, direct-to-cloud model, 1 GiB data set backup results

IBM Cloud Object Storage	Data deduplication %	MiB/s	TiB/hour	TiB per 8 hours	TiB per 10 hours

Cross Regional	50%	1137.8	3.91	31.3	39.1
Regional	50%	1106.0	3.80	30.4	38.0

Table 30: IBM Cloud, small configuration, direct-to-cloud model, 1 GiB data set restore results

Sessions	Cross Regional MiB/s	Cross Regional GiB/hour	Regional MiB/s	Regional GiB/hour
1	73.2	257.3	160.7	565.1
2	118.2	415.4	273.2	960.3
3	179.7	631.8	461.0	1620.8
4	186.8	656.6	536.2	1885.1
5	217.2	763.5	635.7	2235.0
6	223.5	785.8	773.2	2718.2
7	228.3	802.7	491.8	1728.9
8	212.6	747.5	740.1	2602.0
9	250.1	879.4	517.9	1820.7
10	243.4	855.9	529.4	1861.3

3.2.4 IBM Cloud: Extra-Small Instance Measurements for the Direct-to-Cloud Model

128 MiB VE-like front-end data set results (at 5 front-end sessions):

Table 31: IBM Cloud, extra-small configuration, direct-to-cloud model, 128 MiB VE-like data set backup results

IBM Cloud Object Storage	Data deduplication %	MiB/s	GiB/hour	TiB per 8 hours	TiB per 10 hours
Regional	70%	193.4	680.0	5.3	6.6

128 MiB random front-end data set results:

Table 32: IBM Cloud, extra-small configuration, direct-to-cloud model, 128 MiB random data set backup results

IBM Cloud Object Storage	Data deduplication %	MiB/s	GiB/hour	TiB per 8 hours	TiB per 10 hours
Regional	0%	88.7	311.7	2.4	3.0

Table 33: IBM Cloud, extra-small configuration, direct-to-cloud model, 128 MiB random data set restore

Sessions	Regional MiB/s	Regional GiB/hour
1	45.7	160.8
2	68.6	241.1
4	75.7	266.2

1 GiB front-end data set results:

Table 34: IBM Cloud, extra-small configuration, direct-to-cloud model, 1 GiB data set backup results

IBM Cloud Object Storage	Data deduplication %	MiB/s	GiB/hour	TiB per 8 hours	TiB per 10 hours
Regional	50%	136.7	480.8	3.7	4.7

3.2.5 IBM Cloud: Medium Instance Measurements for Disk-to-Cloud Tiering

The following data was restored from the operational recovery directory-container storage pool disk tier.

128 MiB VE-like front-end data set results:

Table 35: IBM Cloud, medium configuration, disk-to-cloud tiering, 128 MiB VE-like data set restore from disk tier

Sessions	MiB/s	TiB/hour
1	259.8	0.89
5	1297.4	4.45
10	2304.0	7.91
15	3456.0	11.87
20	4505.1	15.46
25	5540.8	19.02

128 MiB random front-end data set results:

Table 36: IBM Cloud, medium configuration, disk-to-cloud tiering, 128 MiB random data set restore from disk tier

Sessions	MiB/s	TiB/hour
1	257.3	0.88
5	1054.6	3.62
10	996.0	3.42
15	1080.4	3.71
20	1074.6	3.69
25	1071.2	3.68

1 GiB front-end data set results:

Table 37: IBM Cloud, medium configuration, disk-to-cloud tiering, 1 GiB data set restore results from disk tier

Sessions	MiB/s	TiB/hour
1	247.0	0.85
5	1160.0	4.33
10	2111.9	7.25
15	3004.6	10.32
20	4006.1	13.75
25	4841.3	16.62

3.2.6 IBM Cloud: Small Instance Measurements for Disk-to-Cloud Tiering

The following data was restored from the operational recovery directory-container storage pool disk tier.

128 MiB VE-like front-end data set results

Table 38: IBM Cloud, small configuration, disk-to-cloud tiering, 128 MiB VE-like data set restore from disk tier

Sessions	MiB/s	TiB/hour
1	252.0	0.87
5	1251.0	4.29
10	2377.1	8.16

128 MiB random front-end data set results:

Table 39: IBM Cloud, small configuration, disk-to-cloud tiering, 128 MiB random data set restore from disk tier

Sessions	MiB/s	TiB/hour
1	232.4	0.80
5	591.9	2.03
10	689.0	2.37

1 GiB front-end data set results:

Table 40: IBM Cloud, small configuration, disk-to-cloud tiering, 1 GiB data set restore results from disk tier

Sessions	MiB/s	TiB/hour
1	242.1	0.83
5	1205.1	4.14
10	2235.6	7.68

Appendix

Disk Setup Commands for Linux Deployments

For IBM Spectrum Protect deployments on IBM Cloud, the preferred operating system is Linux, either the latest IBM Spectrum Protect supported Red Hat Enterprise Linux or Ubuntu Linux. With Ubuntu Linux, care should be taken to ensure that all required Linux packages are installed to enable LVM functionality if this component is required (for example: with disk-to-cloud tiering configurations). For more information about the operating systems, see the IBM Spectrum Protect technote (References [3]).

This chapter provides reference information for deployments of IBM Spectrum Protect with Red Hat Enterprise Linux for the large, medium, and small environments. In this case, Red Hat Enterprise Linux was installed on each instance on the IBM Cloud bare metal servers. For the extra-small environment, Ubuntu Linux was used to maximize cost savings. The following sections outline the disk, file system, and miscellaneous commands that were executed in preparation for installing IBM Spectrum Protect.

If you use Linux LVM to share physical volumes for the purposes of a directory-container storage pool disk tier (or cloud accelerator cache), ensure that **LVM striping** is used with the `lvcreate` command such that logical volumes make use of data stripes from all physical disks in the volume group. The number of stripes that you specify when creating a logical volume should match the number of physical disks in the volume group. Lab testing indicates that a suitable stripe size for directory-container storage pool disk tier, cloud accelerator cache, and archive log purposes is **16 KiB**. For example, for a cloud accelerator cache volume group making use of two physical disks, you could use the following command:

```
lvcreate --stripes 2 --stripesize 16 --extents 100%FREE --name sp_cc_vg sp_cc
```

IBM Spectrum Protect, large IBM Cloud system, Red Hat Enterprise Linux:

```
#############################################

#   Miscellaneous

#############################################


# Update and install Yum packages

yum update

yum install -y sg3_utils.x86_64

yum install -y dstat.noarch

yum install -y ftp

yum install -y perl
```

```
yum install -y sysstat

# Set server hostname
hostnamectl set-hostname <desired hostname>

# Set vm.swappiness to 5 to match v4.1 xLinux blueprint guidelines
sysctl vm.swappiness=5

# Install the Korn shell
yum install -y ksh.x86_64

# Disable SELinux
vi /etc/sysconfig/selinux

# Reboot the system

#############################################
#   Disk Setup (Red Hat EL)
#   *** Direct-to-cloud Variation ***
#############################################

# Run the following as the "root" user

# Make the required directories
mkdir /sp
mkdir /sp/sp_db1
mkdir /sp/sp_db2
mkdir /sp/sp_db3
mkdir /sp/sp_db4
mkdir /sp/sp_db5
mkdir /sp/sp_db6
mkdir /sp/sp_db7
mkdir /sp/sp_db8
mkdir /sp/sp_dbb1
mkdir /sp/sp_alog
```

```
mkdir /sp/sp_archlog

mkdir /sp/sp_cc


# Note that disk name values may be different from those seen here in actual
deployments


# Note: Disks may come provisioned into partitioned volumes by IBM Cloud and will
need to be erased/cleared first prior to configuration.

# Change the value for the physical disk to match your environment


# DB

# Consider using exact extent values here to split evenly into 8 volumes

# Change the value for the physical disk to match your environment

pvcreate -f /dev/sdb

vgcreate sp_db /dev/sdb

lvcreate -y --stripes 1 --stripesize 16 --extents 12%FREE --name sp_db1 sp_db

lvcreate -y --stripes 1 --stripesize 16 --extents 12%FREE --name sp_db2 sp_db

lvcreate -y --stripes 1 --stripesize 16 --extents 12%FREE --name sp_db3 sp_db

lvcreate -y --stripes 1 --stripesize 16 --extents 12%FREE --name sp_db4 sp_db

lvcreate -y --stripes 1 --stripesize 16 --extents 12%FREE --name sp_db5 sp_db

lvcreate -y --stripes 1 --stripesize 16 --extents 12%FREE --name sp_db6 sp_db

lvcreate -y --stripes 1 --stripesize 16 --extents 12%FREE --name sp_db7 sp_db

lvcreate -y --stripes 1 --stripesize 16 --extents 12%FREE --name sp_db8 sp_db

mount /dev/mapper/sp_db-sp_db1 /sp/sp_db1

mount /dev/mapper/sp_db-sp_db2 /sp/sp_db2

mount /dev/mapper/sp_db-sp_db3 /sp/sp_db3

mount /dev/mapper/sp_db-sp_db4 /sp/sp_db4

mount /dev/mapper/sp_db-sp_db5 /sp/sp_db5

mount /dev/mapper/sp_db-sp_db6 /sp/sp_db6

mount /dev/mapper/sp_db-sp_db7 /sp/sp_db7

mount /dev/mapper/sp_db-sp_db8 /sp/sp_db8


# Actlog

mkfs.ext4 -F /dev/sdc

mount /dev/sdc /sp/sp_db1


# DB backup

mkfs.ext4 /dev/sdd

mount /dev/sdd /sp/sp_dbb1
```

```
# Archive log
mkfs.ext4 /dev/sde
mount /dev/sde /sp/sp_archlog

# Cloud Accelerator Cache
mkfs.xfs /dev/sdf
mount /dev/sdf /sp/sp_cc

# Edit /etc/fstab to ensure that mount points will be restored on reboot
vi /etc/fstab

#############################################
#   Disk Setup (Red Hat EL)
#   *** Disk-to-cloud Tiering Variation ***
#############################################

# Run the following as the "root" user

# Install LVM for Red Hat
yum install -y lvm2

# Make the required directories
mkdir /sp
mkdir /sp/sp_db1
mkdir /sp/sp_db2
mkdir /sp/sp_db3
mkdir /sp/sp_db4
mkdir /sp/sp_db5
mkdir /sp/sp_db6
mkdir /sp/sp_db7
mkdir /sp/sp_db8
mkdir /sp/sp_alog
mkdir /sp/sp_archlog
mkdir /sp/sp_dbb1
```

```
mkdir /sp/sp_dbb1

mkdir /sp/sp_stg1

mkdir /sp/sp_stg2


# Note that disk name values may be different from those seen here in actual
deployments


# Note: Disks may come provisioned into partitioned volumes by IBM Cloud and will
need to be erased/cleared first prior to configuration.

# Change the value for the physical disk to match your environment


# DB

# Consider using exact extent values here to split evenly into 8 volumes

pvcreate -f /dev/sdb

vgcreate sp_db /dev/sdb

lvcreate -y --stripes 1 --stripesize 16 --extents 12%FREE --name sp_db1 sp_db

lvcreate -y --stripes 1 --stripesize 16 --extents 12%FREE --name sp_db2 sp_db

lvcreate -y --stripes 1 --stripesize 16 --extents 12%FREE --name sp_db3 sp_db

lvcreate -y --stripes 1 --stripesize 16 --extents 12%FREE --name sp_db4 sp_db

lvcreate -y --stripes 1 --stripesize 16 --extents 12%FREE --name sp_db5 sp_db

lvcreate -y --stripes 1 --stripesize 16 --extents 12%FREE --name sp_db6 sp_db

lvcreate -y --stripes 1 --stripesize 16 --extents 12%FREE --name sp_db7 sp_db

lvcreate -y --stripes 1 --stripesize 16 --extents 12%FREE --name sp_db8 sp_db

mount /dev/mapper/sp_db-sp_db1 /sp/sp_db1

mount /dev/mapper/sp_db-sp_db2 /sp/sp_db2

mount /dev/mapper/sp_db-sp_db3 /sp/sp_db3

mount /dev/mapper/sp_db-sp_db4 /sp/sp_db4

mount /dev/mapper/sp_db-sp_db5 /sp/sp_db5

mount /dev/mapper/sp_db-sp_db6 /sp/sp_db6

mount /dev/mapper/sp_db-sp_db7 /sp/sp_db7

mount /dev/mapper/sp_db-sp_db8 /sp/sp_db8


# Actlog

mkfs.ext4 -F /dev/sdc

mount /dev/sdc /sp/sp_db1


# 2x 72.8 TB disks for shared use as DB backup, Archive log, and Disk tier storage

pvcreate -f /dev/sdd

pvcreate -f /dev/sde
```

```
# Create a separate Volume Group for each PV
vgcreate sp_stg1 /dev/sdd
vgcreate sp_stg2 /dev/sde

# Create a DBB volume on each VG
lvcreate -y --stripes 1 --stripesize 16 --size 8T --name sp_dbb1 sp_stg1
lvcreate -y --stripes 1 --stripesize 16 --size 8T --name sp_dbb2 sp_stg2

# Create an archive log volume on the first VG
lvcreate -y --stripes 1 --stripesize 16 --size 4T --name sp_archlog sp_stg1

# Create a Tier Disk storage pool file system on each VG with the remaining space
lvcreate -y --stripes 1 --stripesize 16 --extents 100%FREE --name sp_stg_vol1
sp_stg1
lvcreate -y --stripes 1 --stripesize 16 --extents 100%FREE --name sp_stg_vol2
sp_stg2

# DB backup file systems
mkfs.ext4 /dev/mapper/sp_stg1-sp_dbb1
mkfs.ext4 /dev/mapper/sp_stg2-sp_dbb2
mount /dev/mapper/sp_stg1-sp_dbb1 /sp/sp_dbb1
mount /dev/mapper/sp_stg2-sp_dbb2 /sp/sp_dbb2

# Archive log file system
mkfs.ext4 /dev/mapper/sp_stg1-sp_archlog
mount /dev/mapper/sp_stg1-sp_archlog /sp/sp_archlog

# Disk Tier, Directory Container Storage Pool file system
mkfs.xfs -f /dev/mapper/sp_stg1-sp_stg_vol1
mkfs.xfs -f /dev/mapper/sp_stg2-sp_stg_vol2
mount /dev/mapper/sp_stg1-sp_stg_vol1 /sp/sp_stg1
mount /dev/mapper/sp_stg2-sp_stg_vol2 /sp/sp_stg2

# Edit /etc/fstab to ensure that mount points will be restored on reboot
vi /etc/fstab
```

```
############################################
#   Instance User Setup
############################################

# Run the following as the "root" user.
# Add a Linux group and user to own the IBM Spectrum Protect instance.
# Set the password for this instance.
groupadd tsmsrvrs
useradd -g tsmsrvrs tsminst1
passwd tsminst1

# Ensure that this user can use the mount points previously created
chown -R tsminst1:tsmsrvrs /sp/

# From here, proceed with the IBM Spectrum Protect installation and setup
```

IBM Spectrum Protect, medium IBM Cloud System, Red Hat Enterprise Linux:

```
############################################
#   Miscellaneous
############################################

# Update and install Yum packages
yum update
yum install -y sg3_utils.x86_64
yum install -y dstat.noarch
yum install -y ftp
yum install -y perl
yum install -y sysstat

# Set server hostname
hostnamectl set-hostname <desired hostname>

# Set vm.swappiness to 5 to match v4.1 xLinux Blueprint guidelines
sysctl vm.swappiness=5

# Install the Korn shell
```

```
yum install -y ksh.x86_64

# Disable SELinux
vi /etc/sysconfig/selinux

# Reboot the system

#############################################
#   Disk Setup (Red Hat EL)
#   *** Direct-to-cloud Variation ***
#############################################

# Run the following as the "root" user

# Make the required directories
mkdir /sp
mkdir /sp/sp_db1
mkdir /sp/sp_db2
mkdir /sp/sp_db3
mkdir /sp/sp_db4
mkdir /sp/sp_dbb1
mkdir /sp/sp_alog
mkdir /sp/sp_archlog
mkdir /sp/sp_cc

# Note that disk name values may be different from those seen here in actual deployments
# Change the value for the physical disk to match your environment

# Note: Disks may come provisioned into partitioned volumes by IBM Cloud and will need to be erased/cleared first prior to configuration.

# DB
pvcreate -f /dev/sdb
vgcreate sp_db /dev/sdb
lvcreate -y --stripes 1 --stripesize 16 --extents 25%FREE --name sp_db1 sp_db
```

```
lvcreate -y --stripes 1 --stripesize 16 --extents 25%FREE --name sp_db2 sp_db
lvcreate -y --stripes 1 --stripesize 16 --extents 25%FREE --name sp_db3 sp_db
lvcreate -y --stripes 1 --stripesize 16 --extents 25%FREE --name sp_db4 sp_db
mount /dev/mapper/sp_db-sp_db1 /sp/sp_db1
mount /dev/mapper/sp_db-sp_db2 /sp/sp_db2
mount /dev/mapper/sp_db-sp_db3 /sp/sp_db3
mount /dev/mapper/sp_db-sp_db4 /sp/sp_db4

# Actlog
mkfs.ext4 -F /dev/sdc
mount /dev/sdc /sp/sp_db1

# DB backup
mkfs.ext4 /dev/sdd
mount /dev/sdd /sp/sp_dbb1

# Archive log
mkfs.ext4 /dev/sde
mount /dev/sde /sp/sp_archlog

# Cloud Accelerator Cache
mkfs.xfs /dev/sdf
mount /dev/sdf /sp/sp_cc

# Edit /etc/fstab to ensure that mount points will be restored on reboot
vi /etc/fstab

#############################################
#   Disk Setup (Red Hat EL)
#   *** Disk-to-cloud Tiering Variation ***
#############################################

# Run the following as the "root" user

# Install LVM for Red Hat
yum install -y lvm2

# Make the required directories
```

```
mkdir /sp
mkdir /sp/sp_db1
mkdir /sp/sp_db2
mkdir /sp/sp_db3
mkdir /sp/sp_db4
mkdir /sp/sp_alog
mkdir /sp/sp_archlog
mkdir /sp/sp_dbb1
mkdir /sp/sp_dbb1
mkdir /sp/sp_stg1

# Note that disk name values may be different from those seen here in actual
deployments

# Note: Disks may come provisioned into partitioned volumes by IBM Cloud and will
need to be erased/cleared first prior to configuration.
# Change the value for the physical disk to match your environment

# DB
pvcreate -f /dev/sdb
vgcreate sp_db /dev/sdb
lvcreate -y --stripes 1 --stripesize 16 --extents 25%FREE --name sp_db1 sp_db
lvcreate -y --stripes 1 --stripesize 16 --extents 25%FREE --name sp_db2 sp_db
lvcreate -y --stripes 1 --stripesize 16 --extents 25%FREE --name sp_db3 sp_db
lvcreate -y --stripes 1 --stripesize 16 --extents 25%FREE --name sp_db4 sp_db
mount /dev/mapper/sp_db-sp_db1 /sp/sp_db1
mount /dev/mapper/sp_db-sp_db2 /sp/sp_db2
mount /dev/mapper/sp_db-sp_db3 /sp/sp_db3
mount /dev/mapper/sp_db-sp_db4 /sp/sp_db4

# Actlog
mkfs.ext4 -F /dev/sdc
mount /dev/sdc /sp/sp_db1

# 90.88 TB disk for shared use as DB backup, Archive log, and Disk tier storage
pvcreate -f /dev/sdd
```

```
vgcreate sp_stg1 /dev/sdd

# Create two 4 TB DBB volumes
lvcreate -y --stripes 1 --stripesize 16 --size 4T --name sp_dbb1 sp_stg1
lvcreate -y --stripes 1 --stripesize 16 --size 4T --name sp_dbb2 sp_stg1

# Create a 3 TB archive log volume
lvcreate -y --stripes 1 --stripesize 16 --size 3T --name sp_archlog sp_stg1

# Create a Tier Disk storage pool volume with the remaining space
lvcreate -y --stripes 1 --stripesize 16 --extents 100%FREE --name sp_stg_vol1
sp_stg1

# DB backup file systems
mkfs.ext4 /dev/mapper/sp_stg1-sp_dbb1
mkfs.ext4 /dev/mapper/sp_stg1-sp_dbb2
mount /dev/mapper/sp_stg1-sp_dbb1 /sp/sp_dbb1
mount /dev/mapper/sp_stg1-sp_dbb2 /sp/sp_dbb2

# Archive log file system
mkfs.ext4 /dev/mapper/sp_stg1-sp_archlog
mount /dev/mapper/sp_stg1-sp_archlog /sp/sp_archlog

# Disk Tier, Directory Container Storage Pool file system
mkfs.xfs -f /dev/mapper/sp_stg1-sp_stg_vol1
mount /dev/mapper/sp_stg1-sp_stg_vol1 /sp/sp_stg1

# Edit /etc/fstab to ensure that mount points will be restored on reboot
vi /etc/fstab


#############################################
#   Instance User Setup
#############################################

# Run the following as the "root" user.
# Add a Linux group and user to own the IBM Spectrum Protect instance.
# Set the password for this instance.
groupadd tsmsrvrs
```

```
useradd -g tsmsrvrs tsminst1
passwd tsminst1

# Ensure that this user can use the mount points previously created
chown -R tsminst1:tsmsrvrs /sp/

# From here, proceed with the IBM Spectrum Protect installation and setup
```

IBM Spectrum Protect, small IBM Cloud System, Red Hat Enterprise Linux:

```
#############################################
#   Miscellaneous
#############################################

# Update and install Yum packages
yum update
yum install -y sg3_utils.x86_64
yum install -y dstat.noarch
yum install -y ftp
yum install -y perl
yum install -y sysstat

# Set server hostname
hostnamectl set-hostname <desired hostname>

# Set vm.swappiness to 5 to match v4.1 xLinux blueprint guidelines
sysctl vm.swappiness=5

# Install the Korn shell
yum install -y ksh.x86_64

# Disable SELinux
vi /etc/sysconfig/selinux

# Reboot the system
```

```
#############################################
#   Disk Setup (Red Hat EL)
#   *** Direct-to-cloud Variation ***
#############################################

# Run the following as the "root" user

# Make the required directories
mkdir /sp
mkdir /sp/sp_db1
mkdir /sp/sp_db2
mkdir /sp/sp_db3
mkdir /sp/sp_db4
mkdir /sp/sp_dbb1
mkdir /sp/sp_alog
mkdir /sp/sp_archlog
mkdir /sp/sp_cc

# Note that disk name values may be different from those seen here in actual
deployments
# Change the value for the physical disk to match your environment

# Note: Disks may come provisioned into partitioned volumes by IBM Cloud and will
need to be erased/cleared first prior to configuration.

# DB
pvcreate -f /dev/sdb
vgcreate sp_db /dev/sdb
lvcreate -y --stripes 1 --stripesize 16 --extents 50%FREE --name sp_db1 sp_db
lvcreate -y --stripes 1 --stripesize 16 --extents 50%FREE --name sp_db2 sp_db
mount /dev/mapper/sp_db-sp_db1 /sp/sp_db1
mount /dev/mapper/sp_db-sp_db2 /sp/sp_db2

# Actlog
mkfs.ext4 -F /dev/sdc
mount /dev/sdc /sp/sp_db1

# DB backup
mkfs.ext4 /dev/sdd
```

```
mount /dev/sdd /sp/sp_dbb1

# Archive log
mkfs.ext4 /dev/sde
mount /dev/sde /sp/sp_archlog

# Cloud Accelerator Cache
mkfs.xfs /dev/sdf
mount /dev/sdf /sp/sp_cc

# Edit /etc/fstab to ensure that mount points will be restored on reboot
vi /etc/fstab

#############################################
#   Disk Setup (Red Hat EL)
#   *** Disk-to-cloud Tiering Variation ***
#############################################

# Run the following as the "root" user

# Install LVM for Red Hat
yum install -y lvm2

# Make the required directories
mkdir /sp
mkdir /sp/sp_db1
mkdir /sp/sp_db2
mkdir /sp/sp_alog
mkdir /sp/sp_archlog
mkdir /sp/sp_dbb1
mkdir /sp/sp_dbb2
mkdir /sp/sp_stg1

# Note that disk name values may be different from those seen here in actual
deployments
```

```
# Note: Disks may come provisioned into partitioned volumes by IBM Cloud and will
need to be erased/cleared first prior to configuration.

# Change the value for the physical disk to match your environment


# DB

pvcreate -f /dev/sdb

vgcreate sp_db /dev/sdb

lvcreate -y --stripes 1 --stripesize 16 --extents 50%FREE --name sp_db1 sp_db

lvcreate -y --stripes 1 --stripesize 16 --extents 50%FREE --name sp_db2 sp_db

mount /dev/mapper/sp_db-sp_db1 /sp/sp_db1

mount /dev/mapper/sp_db-sp_db2 /sp/sp_db2


# Actlog

mkfs.ext4 -F /dev/sdc

mount /dev/sdc /sp/sp_db1


# 90.88 TB disk for shared use as DB backup, Archive log, and Disk tier storage

pvcreate -f /dev/sdd

vgcreate sp_stg1 /dev/sdd


# Create two 2 TB DBB volumes

lvcreate -y --stripes 1 --stripesize 16 --size 2T --name sp_dbb1 sp_stg1

lvcreate -y --stripes 1 --stripesize 16 --size 2T --name sp_dbb2 sp_stg1


# Create a 1 TB archive log volume

lvcreate -y --stripes 1 --stripesize 16 --size 1T --name sp_archlog sp_stg1


# Create a Tier Disk storage pool volume with the remaining space

lvcreate -y --stripes 1 --stripesize 16 --extents 100%FREE --name sp_stg_vol1
sp_stg1


# DB backup file systems

mkfs.ext4 /dev/mapper/sp_stg1-sp_dbb1

mkfs.ext4 /dev/mapper/sp_stg1-sp_dbb2

mount /dev/mapper/sp_stg1-sp_dbb1 /sp/sp_dbb1

mount /dev/mapper/sp_stg1-sp_dbb2 /sp/sp_dbb2


# Archive log file system

mkfs.ext4 /dev/mapper/sp_stg1-sp_archlog
```

```
mount /dev/mapper/sp_stg1-sp_archlog /sp/sp_archlog

# Disk Tier, Directory Container Storage Pool file system
mkfs.xfs -f /dev/mapper/sp_stg1-sp_stg_vol1
mount /dev/mapper/sp_stg1-sp_stg_vol1 /sp/sp_stg1

# Edit /etc/fstab to ensure that mount points will be restored on reboot
vi /etc/fstab

#############################################
#   Instance User Setup
#############################################

# Run the following as the "root" user.
# Add a Linux group and user to own the IBM Spectrum Protect instance.
# Set the password for this instance.
groupadd tsmsrvrs
useradd -g tsmsrvrs tsminst1
passwd tsminst1

# Ensure that this user can use the mount points previously created
chown -R tsminst1:tsmsrvrs /sp/

# From here, proceed with the IBM Spectrum Protect installation and setup
```

IBM Spectrum Protect, extra-small IBM Cloud System, Ubuntu Linux:

```
#############################################
#   Miscellaneous
#############################################

# Update apt packages, install tooling
apt update
apt upgrade -y
apt install scsitools -y
apt install dstat -y
```

```
apt install sysstat -y
apt install multipath-tools -y
apt install multipath-tools-boot -y

# Start the multipath daemon
touch /etc/multipath.conf
systemctl restart multipath-tools.service

# Set server hostname
hostnamectl set-hostname <desired hostname>

# Set vm.swappiness to 5 to match v4.1 xLinux blueprint guidelines
sysctl vm.swappiness=5

# Install the Korn shell
apt install ksh -y

# Install LVM for Ubuntu
apt install lvm2 -y
systemctl enable lvm2-lvmetad
systemctl start lvm2-lvmetad

# Reboot the system

# Run the following as the "root" user

# Make the required directories
mkdir /sp
mkdir /sp/sp_db1
mkdir /sp/sp_db2
mkdir /sp/sp_db3
mkdir /sp/sp_db4
mkdir /sp/sp_dbb1
mkdir /sp/sp_alog
mkdir /sp/sp_archlog
mkdir /sp/sp_cc

# Note that disk name values may be different from those seen here in actual
deployments
```

```
# Note: Disks may come provisioned into partitioned volumes by IBM Cloud and will
need to be erased/cleared first prior to configuration.

# Change the value for the physical disk to match your environment


# Cloud Cache

pvcreate /dev/xvdf

vgcreate sp_cc /dev/xvdf

lvcreate --extents 100%FREE --name sp_cc_vg sp_cc

mkfs.xfs /dev/mapper/sp_cc-sp_cc_vg

mount /dev/mapper/sp_cc-sp_cc_vg /sp/sp_cc


# DB and actlog.

pvcreate /dev/xvdc

vgcreate sp_db /dev/xvdc

lvcreate --extents 15360 --name sp_db_db1 sp_db

lvcreate --extents 15360 --name sp_db_db2 sp_db

lvcreate --extents 15360 --name sp_db_db3 sp_db

lvcreate --extents 15360 --name sp_db_db4 sp_db

lvcreate --extents 15359 --name sp_db_alog sp_db

mkfs.ext4 /dev/mapper/sp_db-sp_db_db1

mkfs.ext4 /dev/mapper/sp_db-sp_db_db2

mkfs.ext4 /dev/mapper/sp_db-sp_db_db3

mkfs.ext4 /dev/mapper/sp_db-sp_db_db4

mkfs.ext4 /dev/mapper/sp_db-sp_db_alog

mount /dev/mapper/sp_db-sp_db_db1 /sp/sp_db1

mount /dev/mapper/sp_db-sp_db_db2 /sp/sp_db2

mount /dev/mapper/sp_db-sp_db_db3 /sp/sp_db3

mount /dev/mapper/sp_db-sp_db_db4 /sp/sp_db4

mount /dev/mapper/sp_db-sp_db_alog /sp/sp_alog


# DB backup and Archive log

pvcreate /dev/xvde

vgcreate sp_archlog_dbb /dev/xvde

lvcreate --extents 50%FREE --name sp_archlog sp_archlog_dbb

lvcreate --extents 100%FREE --name sp_dbb sp_archlog_dbb
```

```
mkfs.ext4 /dev/mapper/sp_archlog_dbb-sp_dbb
mkfs.ext4 /dev/mapper/sp_archlog_dbb-sp_archlog
mount /dev/mapper/sp_archlog_dbb-sp_dbb /sp/sp_dbb1
mount /dev/mapper/sp_archlog_dbb-sp_archlog /sp/sp_archlog

# Edit /etc/fstab to ensure that mount points will be restored on reboot
vi /etc/fstab
```

Disk Benchmarking

As a part of vetting each IBM Cloud system outlined in this document, disk benchmark tests were performed to validate the capability of the disk volumes underlying the IBM Spectrum Protect database, cloud accelerator cache, and directory-container storage pool disk tier. From a database point of view, this vetting was done to ensure that the volumes were sufficiently capable from an IOPS perspective to support the 8 KiB random mixed write and read workload that a busy Blueprint-level system would demand. From a cloud cache standpoint, the vetting was performed to ensure that overlapped 128 - 256 KiB write and read throughput could achieve a rate high enough such that the server's bottleneck for IO would be at the instance-to-object storage network level and not the disk level. The goal was to ensure that the disk could perform at a rate such that the IBM Spectrum Protect server could utilize it during overlapped ingest and be able to stress the network link layer simultaneously. From a directory-container storage pool disk tier point of view, benchmarking was conducted to ensure that this storage location could adequately handle separate daily backup ingestion and cloud transfer responsibilities.

Disk benchmarking was conducted by using the **tsmdiskperf.pl** Perl script, provided as a part of the Blueprint configuration scripts package found on the IBM Spectrum Protect Blueprints page (References [1]). The script was run as follows:

`perl tsmdiskperf.pl workload=stgpool fslist=`*`directory_list`*

`perl tsmdiskperf.pl workload=db fslist=`*`directory_list`*

With a `stgpool` workload specification, the script drives a 256 KiB I/O pattern, whereas with a db workload specification, the script drives 8 KiB operations. For each directory location provided as a value to the comma-separate `fslist`, a pair of I/O processes is created to write and read to test files that are generated in that directory.

Typical script output for a `stgpool` workload run resembles the following example:

```
======================================================================
: IBM Spectrum Protect disk performance test    (Program version 3.1b)
:
: Workload type:                stgpool
```

```
: Number of filesystems:        1
: Mode:                         readwrite
: Files to write per fs:        5
: File size:                    2 GB
:
======================================================================
:
: Beginning I/O test.
: The test can take upwards of ten minutes, please be patient ...
: Starting write thread ID: 1 on filesystem /sp/sp_cc/1
: Starting read thread ID: 2 on filesystem /sp/sp_cc/1
: All threads are finished.  Stopping iostat process with id 111519
===================================================================
:  RESULTS:
:  Devices reported on from  output:
:  dm-2
:
:  Average R Throughput (KB/sec):       19473.92
:  Average W Throughput (KB/sec):       19377.45
:  Avg Combined Throughput (MB/sec):    37.94
:  Max Combined Throughput (MB/sec):    160.57
:
:  Average IOPS:                        464.63
:  Peak IOPS:                           2154.57 at 11/10/2017 04:22:32
:
:  Total elapsed time (seconds):        443
===================================================================
```

The value that was extracted for the purposes of comparison and validation for `stgpool` workloads was `Avg Combined Throughput (MB/sec)`. The goal was to determine the largest aggregate average throughput for writes and reads to the accelerator cache disk such that overlapped backup ingestion and transfer to object storage will not be constrained by disk capability. A similar goal was used for the directory-container storage pool disk tier disk.

When running the tool in `db` workload mode, output is similar to the following example:

```
======================================================================
```

```
: IBM Spectrum Protect disk performance test    (Program version 3.1b)
:
: Workload type:                db
: Number of filesystems:        1
: Mode:                         readwrite
: Thread count per FS:          2
: I/Os per thread:              500000
: File size:                    10 GB
:
======================================================================
:
: Creating files of 10 GB to simulate IBM Spectrum Protect DB.
: Issuing command ./ldeedee if=/dev/zero of=/sp/sp_db1/1/tsmdiskperf_1 bs=1024k
count=10240 dio=2 > /dev/null 2>&1
: Issuing command ./ldeedee if=/dev/zero of=/sp/sp_db1/1/tsmdiskperf_2 bs=1024k
count=10240 dio=2 > /dev/null 2>&1
:
: Beginning I/O test.
: The test can take upwards of ten minutes, please be patient ...
: All threads are finished.  Stopping iostat process with id 111978
===================================================================
:  RESULTS:
:  Devices reported on from  output:
:  dm-6
:
:  Average R Throughput (KB/sec):       12907.53
:  Average W Throughput (KB/sec):       12707.15
:  Avg Combined Throughput (MB/sec):    25.01
:  Max Combined Throughput (MB/sec):    42.70
:
:  Average IOPS:                        3202.28
:  Peak IOPS:                           5465.86 at 11/10/2017 04:31:47
:
:  Total elapsed time (seconds):        30
===================================================================
```

For the db workload tests, the `Avg Combined Throughput (MB/sec)` and `Average IOPS` metrics are significant for evaluating database disk capability. Here, the small random IOPS capability of the underlying disk that is used for the IBM Spectrum Protect Db2 database is of interest.

To conduct measurements of your own, increase the number of write/read threads pairs (and directories) by 1 for each test until the average throughput, the average IOPS, or both stabilize (level off). Benchmark test results are provided here as a reference for those who want to build systems resembling those described in this document and who want to validate that their system is capable of supporting the described level of ingestion. For each graph, the horizontal axis represents the quantity of write/read thread pairs (and the number of directory locations used with `fslist`). For each successive bar to the right, the thread count affecting the disk is increased by 2 (1 write thread, 1 read thread, and adding a directory location). The vertical axis represents total average throughput in MiB/s.

IBM Cloud large configuration

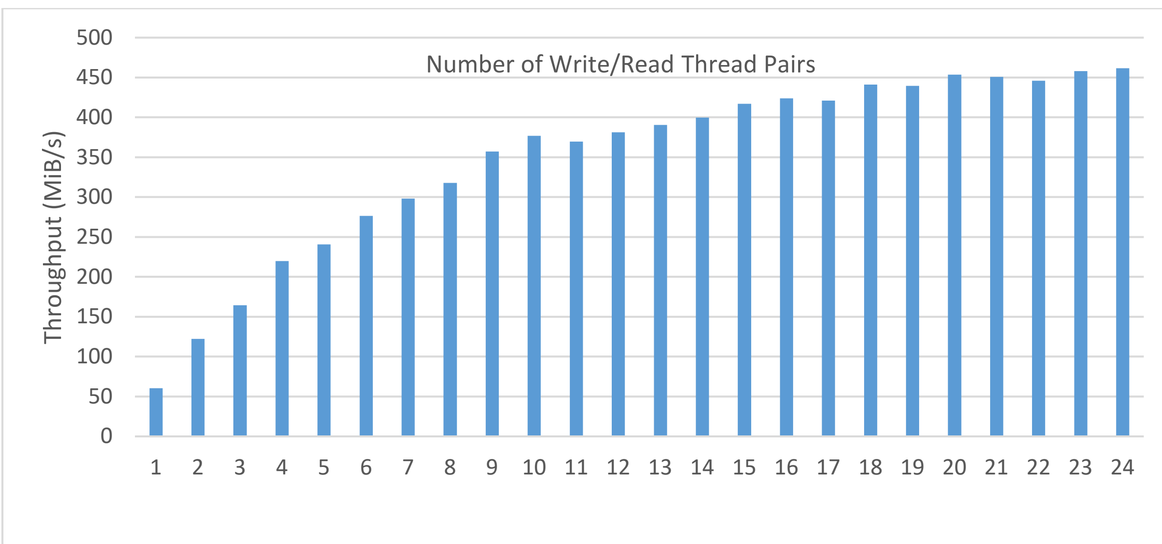


Figure 6: IBM Cloud large configuration; database volume average throughput; 8 KiB random writes/reads

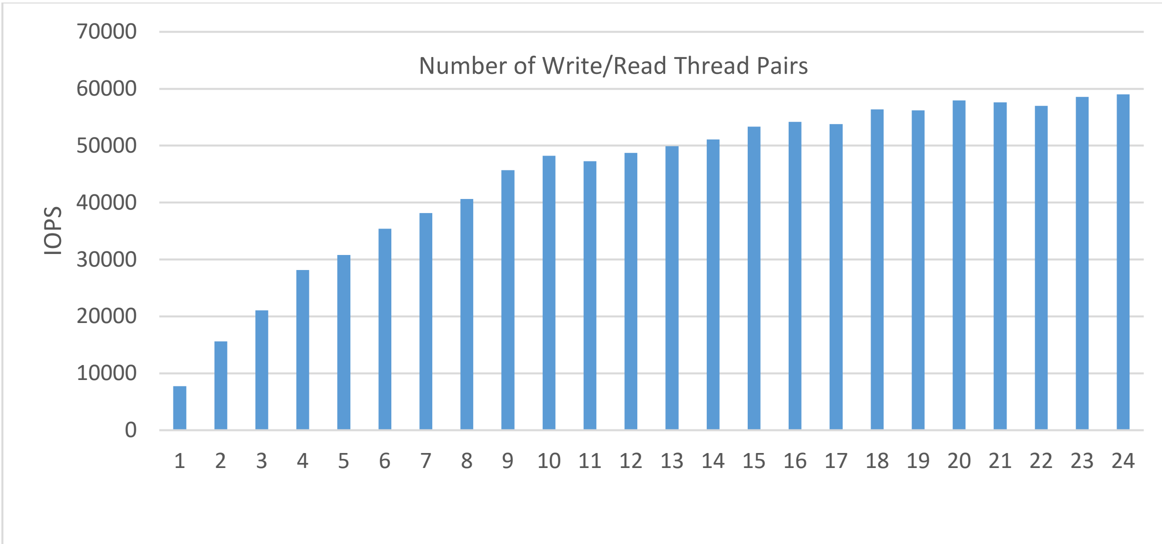


Figure 7: IBM Cloud large configuration; database volume average IOPS; 8 KiB random writes/reads

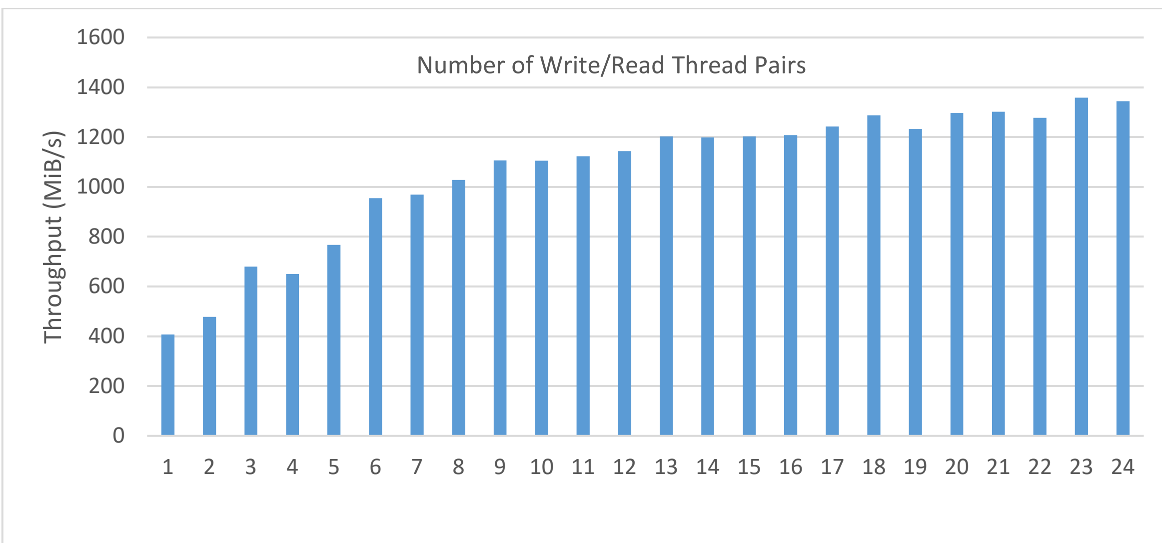


Figure 8: IBM Cloud large configuration; cloud cache volume average throughput; mixed 256 KiB writes and reads

IBM Cloud medium configuration

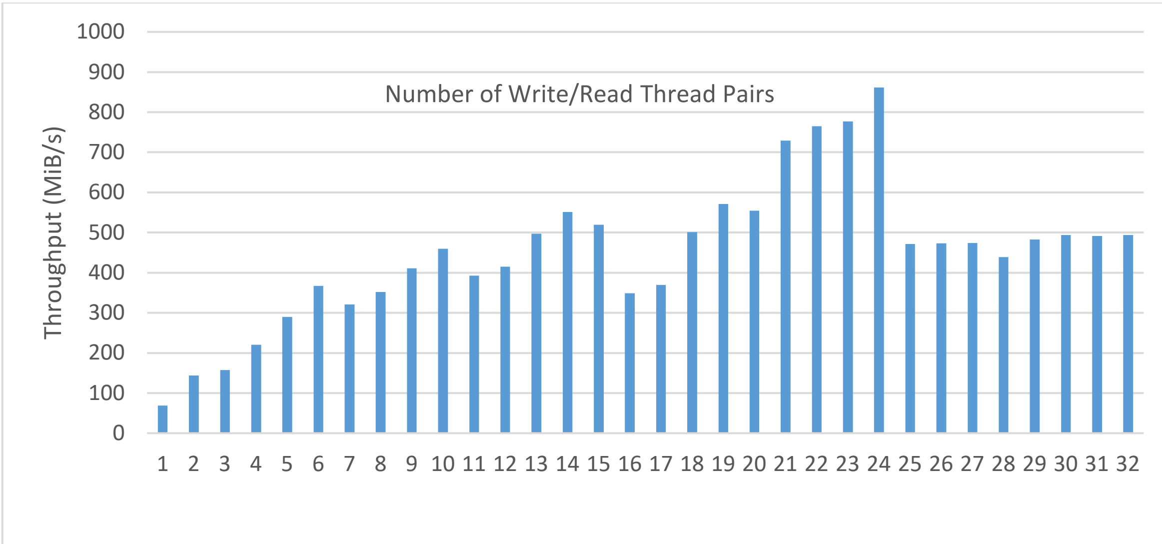


Figure 9: IBM Cloud medium configuration; database volume average throughput; 8 KiB random writes/reads

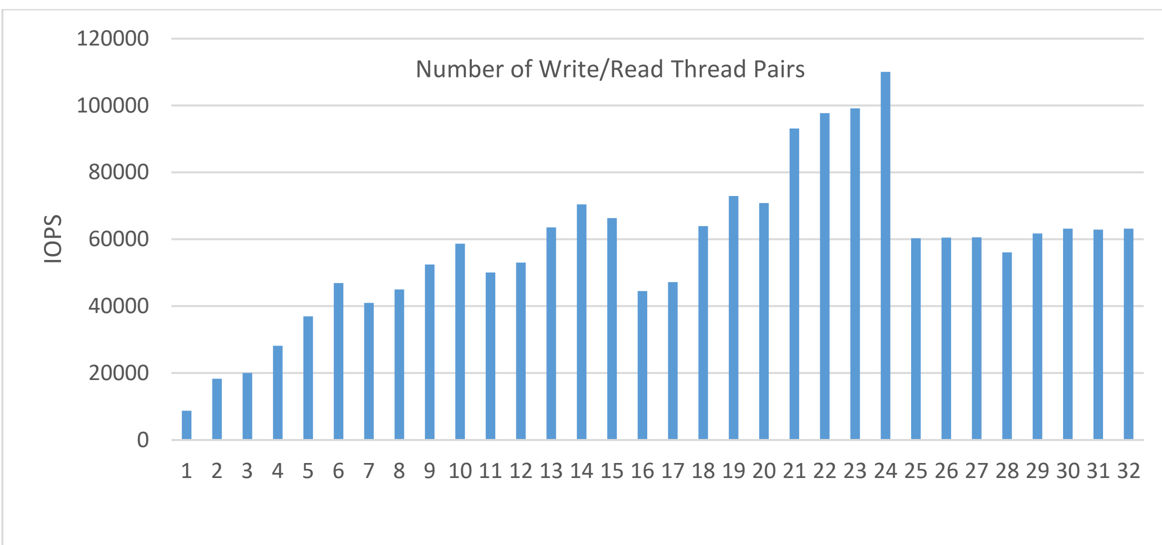


Figure 10: IBM Cloud medium configuration; database volume average IOPS; 8 KiB random writes/reads

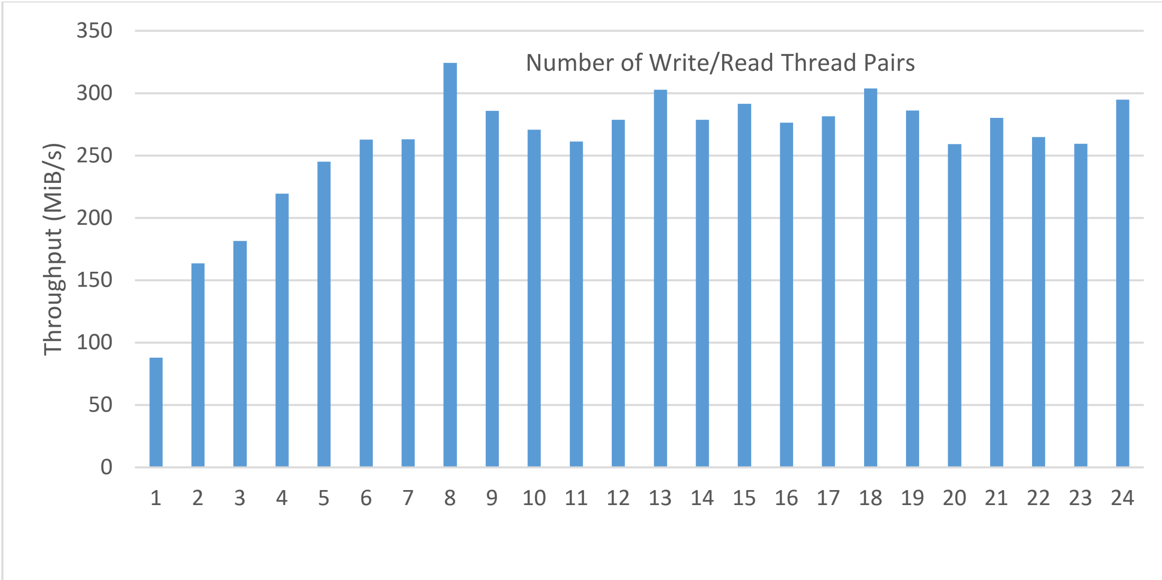


Figure 11: IBM Cloud medium configuration; cloud cache volume average throughput; mixed 256 KiB writes and reads

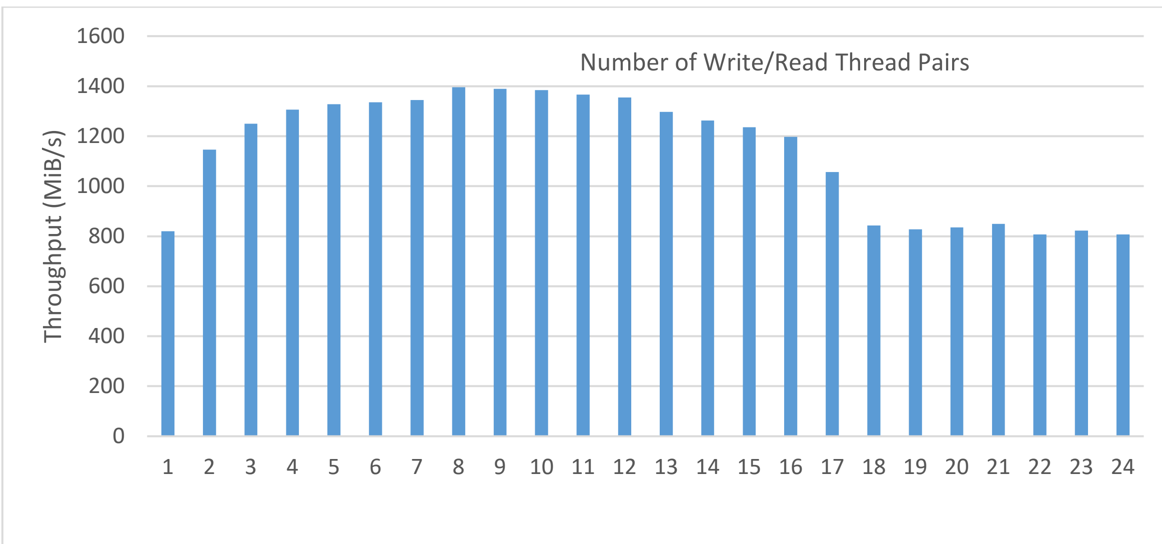


Figure 12: IBM Cloud medium configuration; disk-to-cloud tiering disk tier volume average throughput; mixed 256 KiB writes/reads

IBM Cloud small configuration

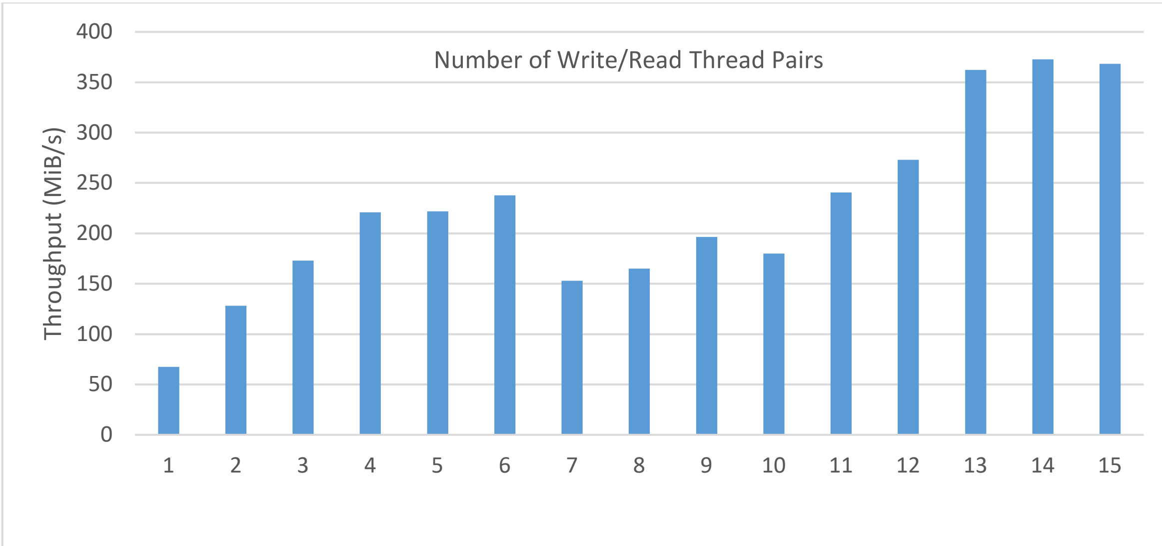


Figure 13: IBM Cloud small configuration; disk-to-cloud tiering disk tier volume average throughput; mixed 256 KiB writes/reads

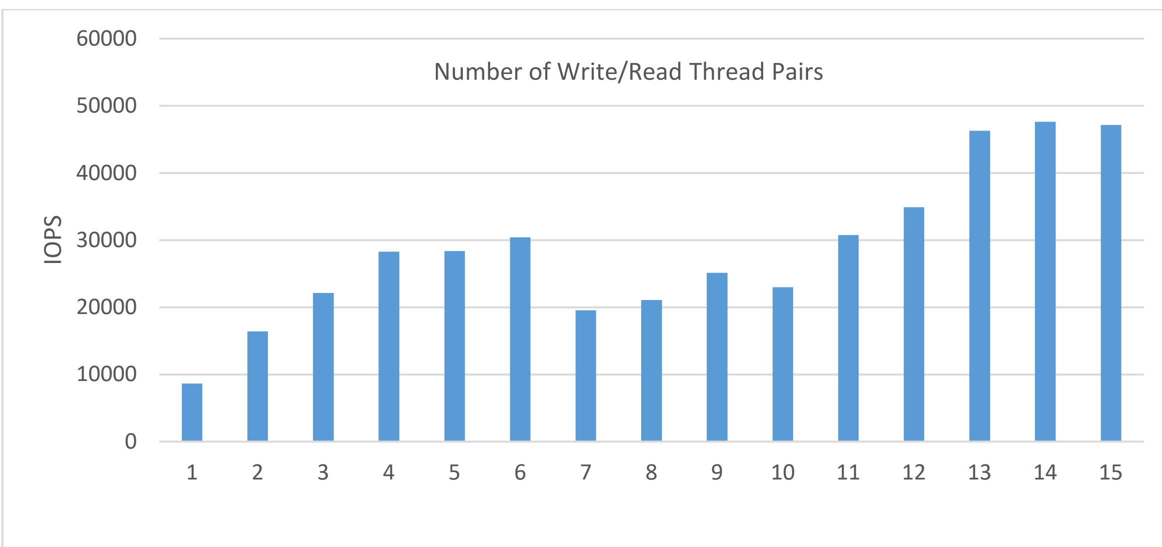


Figure 14: IBM Cloud small configuration; database volume average IOPS; 8 KiB random writes/reads

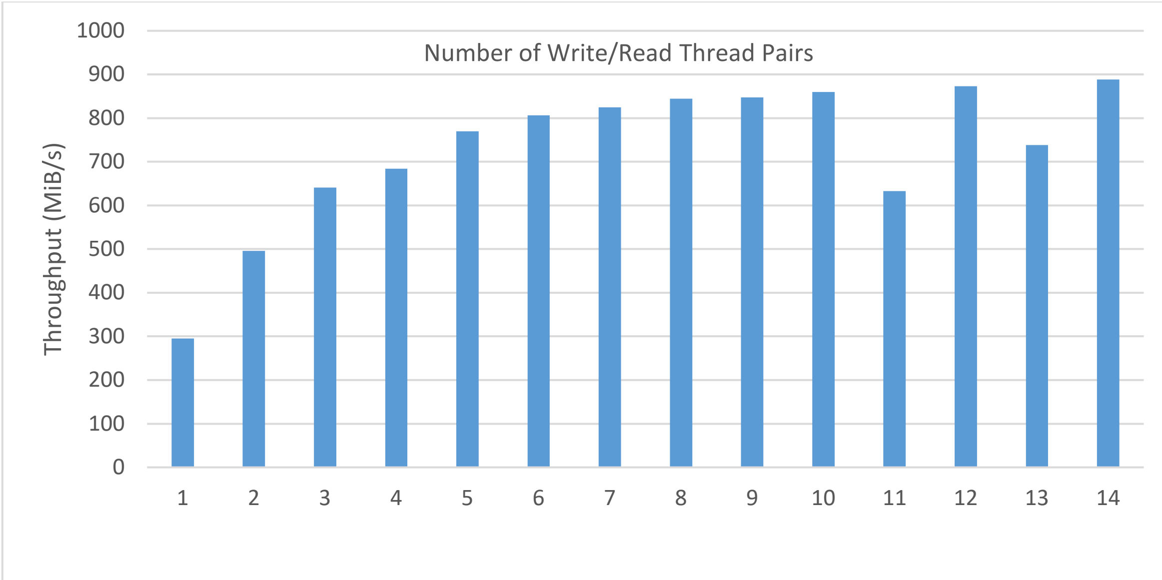


Figure 15: IBM Cloud small configuration; cloud cache volume average throughput; mixed 256 KiB writes/reads

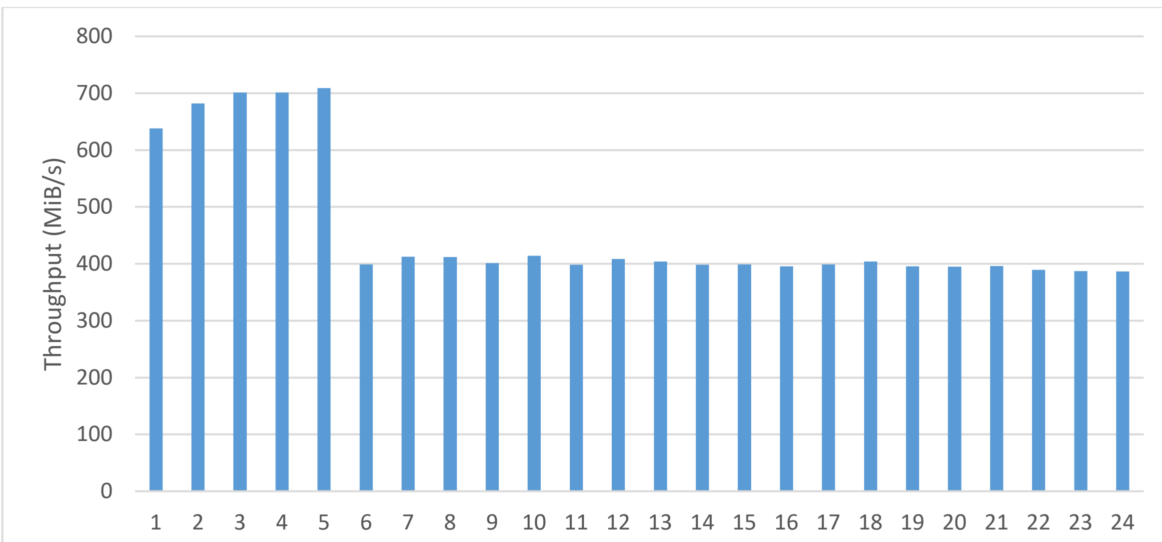


Figure 16: IBM Cloud small configuration; disk-to-cloud tiering disk tier volume average throughput; mixed 256 KiB writes/reads

Object Storage Benchmarking

Another important step in validating the capability of an IBM Cloud-based IBM Spectrum Protect solution is to benchmark the throughput of the bare metal server to IBM Cloud Object Storage with a workload that is typical of IBM Spectrum Protect. Ideally, any in-the-cloud IBM Spectrum Protect solution should be network bound in terms of its connection to object storage. After inline data deduplication, compression, and encryption, the back-end ingestion rate over HTTPS should dictate an upper bound for daily ingestion performance of a system.

To help facilitate this test activity in-house, a Java program was developed by the IBM Spectrum Protect test team to emulate the behavior of the server's use of the IBM Cloud Object Storage API. The tool can be used to drive various backup and restore-type activities to object storage, including direct HTTP PUT, GET, multipart file upload, and range-read restore behavior with a variable number of threads. This tool, known as `SPObjBench.jar`, is included with the Benchmarking package provided with this document.

Also included in the Benchmarking package is a Perl script, `tsmobjperf.pl`, which can be used to automate execution of the `SPObjBench.jar` file with several thread counts to measure ingest (PUT) and restore (GET) scalability.

On the normal ingestion path within the scope of a direct-to-cloud with accelerator cache architecture, the IBM Spectrum Protect server attempts to upload up to 100 1 GB disk container files from the accelerator cache in parallel by using multipart upload. Within a production environment, this work would occur in conjunction with overlapped ingestion to another set of container files within the same storage pool directory locations on accelerator cache disk storage.

To attempt to isolate and gauge the instance-to-object storage ingestion capability of a system, you can complete the following steps:

1) Populate a set of 10 1 GB files in a memory-mapped file system location to use as source data for ingestion. The use of memory-mapped locations (such as `tmpfs` on Linux) is preferred to eliminate source disk bottlenecks. For a Linux system with at least 11 GB of free RAM, run the following commands:

```
mkdir /mnt/ramdisk

mount –t tmpfs –o size=11g tmpfs /mnt/ramdisk

for I in `seq 10`; do dd if=/dev/urandom
of=/mnt/ramdisk/file.$I bs=1048576 count=1024; done
```

2) To run a set of automated tests scaling from 1 to 100 threads, run the `tsmobjperf.pl` tool by using the recently created RAM disk files as source files to upload. If more threads are specified than files are present in the source list, the tool completes a round-robin action over these source files. Because all activity is read-only, using separate file handles from memory-mapped sources, multiple threads sharing the same file is not a concern. To test with 1, 10, 20, 30, 40, 50, 60, 70, 80, 90, and 100 threads, run the tool as follows, specifying the arguments as needed:

```
perl tsmobjperf.pl type=type endpoints=endpoint user="user"
pass="pass" bucket=bucket min=1 max=100 step=10 flist=
comma_delimited_source_files_list
```

where:

- *type* should be `s3` for IBM Cloud Object Storage.
- *endpoint* specifies a comma-delimited list of IP addresses or URLs for the object storage endpoints. For IBM Cloud, this should be a single private IBM Cloud network endpoint that is accessed over HTTPS (for security).
- For S3, the *user* is a public key ID.
- For S3, the *pass* is the secret key for a user who has valid S3 credentials to create buckets and PUT and GET objects in the region indicated by the *endpoint* URL. These values align with those that are used to define an IBM Spectrum Protect cloud-container storage pool, either via the Operations Center or the command line.
- The *bucket* value should be an IBM Cloud Object Storage bucket or vault name that the credentialed user has create/PUT/GET access to and that exists in the object storage system. The *min* and *max* values should indicate the minimum and maximum thread counts to test.
- The *step* value should indicate the increase in thread count from test to test.
- The `flist` parameter should include a comma-delimited list of source files to be used for multipart upload. These files should be the same as those created earlier in the memory-mapped file system.

The following example is for execution to an IBM Cloud Object Storage Regional (South) endpoint, using 100 upload threads with an existing test bucket:

```
perl tsmobjperf.pl type=s3 endpoints=https:// s3.us-
south.objectstorage.service.networklayer.com user=”PUBLICKEYID”
pass=”SECRETKEY” bucket=testbucket min=1 max=100 step=10
flist=/mnt/ramdisk/file.1,/mnt/ramdisk/file.2,/mnt/ramdisk/file.
3,/mnt/ramdisk/file.4,/mnt/ramdisk/file.5,/mnt/ramdisk/file.6,/m
nt/ramdisk/file.7,/mnt/ramdisk/file.8,/mnt/ramdisk/file.9
,/mnt/ramdisk/file.10
```

Each thread count test (for 1, 10, 20, or more threads) will upload 10 x 1 GB objects per thread. The previous example would result in a total of 5510 GB of data being stored to the test bucket after all thread tests are completed. The tool does not remove objects that are created. You must remove the objects manually after test completion.

Upon completion, the tool generates aggregate throughput metrics that can be used to estimate practical instance-to-object storage performance rates for IBM Spectrum Protect. Data is provided in comma-separated-value format (CSV) and the output of the `SPObjBench.jar` tool can be inspected upon completion as well:

```
===================================================================
: IBM Spectrum Protect object storage test
:
: Test Mode:    write
: Type:         s3
: Endpoints:    https://s3.us-south.objectstorage.service.networklayer.com
: User:         PUBLICKEY
: Pass:         SECRETKEY
: Test Bucket:  testbucket
: Min Threads:  1
: Max Threads:  100
: Thread Step:  10
: File List:
/mnt/ramdisk/file.1,/mnt/ramdisk/file.2,/mnt/ramdisk/file.3,/mnt/ramdisk/file.4,
/mnt/ramdisk/file.5,/mnt/ramdisk/file.6,/mnt/ramdisk/file.7,/mnt/ramdisk/file.8,
/mnt/ramdisk/file.9 ,/mnt/ramdisk/file.10
: Using java:   java
===================================================================


SPObjBench.jar output being captured to file:   tsmobjperf.1540336631.out


===================================================================
: Test Results
Thread Count, Write Throughput (MB/s)
1, XXX
10, XXX
20, XXX
30, XXX
40, XXX
50, XXX
60, XXX
70, XXX
80, XXX
90, XXX
100, XXX
===================================================================
```

It can be beneficial to monitor network transmission rates externally from the tool, as well, to validate the absolute throughput rate that is experienced to object storage over the (Ethernet) network. The tool reports an aggregate rate that can include build-up and tear-down overhead associated with the tool. Calculating an actual transmission rate from the instance-to-object storage while the test is running can give an indication of the throughput limits of the environment. On Linux, for example, the `dstat` utility can be used to monitor several system metrics at once, including network interface send and receive statistics, by using the basic command:

```
% dstat

You did not select any stats, using -cdngy by default.

----total-cpu-usage---- -dsk/total- -net/total- ---paging-- ---system--

usr sys idl wai hiq siq| read  writ| recv  send|  in   out | int   csw

  0   0 100   0   0   0|  60B 2511B|   0     0 |   0     0 |  76    71

 15   1  84   0   0   1|   0    24k|1674k   58M|   0     0 |  42k 2785

 15   1  83   0   0   1|   0     0 |1838k   62M|   0     0 |  46k 2969

 16   1  82   0   0   1|   0     0 |1832k   61M|   0     0 |  45k 3127

 15   1  84   0   0   1|   0     0 |1753k   61M|   0     0 |  44k 2822

 16   1  83   0   0   1|   0     0 |1811k   62M|   0     0 |  45k 3001

 15   1  83   0   0   1|   0     0 |1778k   62M|   0     0 |  45k 3068

 16   1  82   0   0   1|   0     0 |1870k   63M|   0     0 |  46k 3068

 16   1  82   0   0   1|   0     0 |1933k   64M|   0     0 |  46k 3011

 15   1  83   0   0   1|   0     0 |1834k   63M|   0     0 |  46k 2974
```

The `dstat` tool generates a new line of metrics at a configured interval, much like the standard `iostat` and `netstat` utilities. In the previous output, the `net/total send` column is of greatest interest, here reported in mebibytes, as an indication of how quickly data could be sent to the object storage endpoint from the server.

Instance and Object Storage: Navigating the IBM Cloud Portal

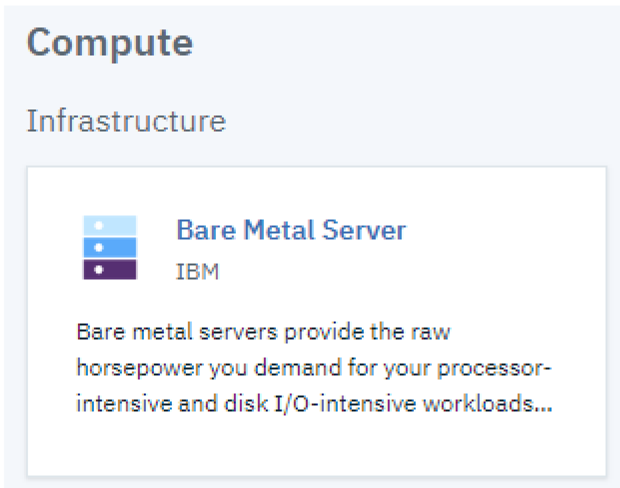
When deploying a new IBM Cloud based IBM Spectrum Protect environment, you must consider tasks such as navigating the IBM Cloud web portal and creating relevant cloud resources. Use the following steps as a starting point for creating IBM Cloud resources. An important consideration when building an IBM Spectrum Protect server in IBM Cloud is to correctly order host servers and object storage such that the private (internal IBM Cloud) network link between these resources is efficient.

Begin by navigating to the IBM Cloud home page and log in with the appropriate user credentials.

IBM Cloud Bare Metal Servers

1. At the top-right corner of the window, click **Create Resource.**

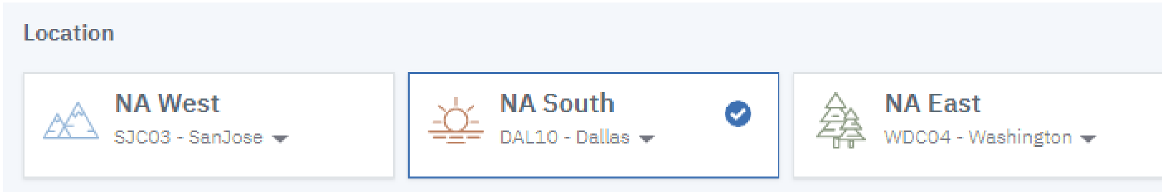
2. Under the **Compute** section and **Infrastructure** subsection, click **Bare Metal Server.**



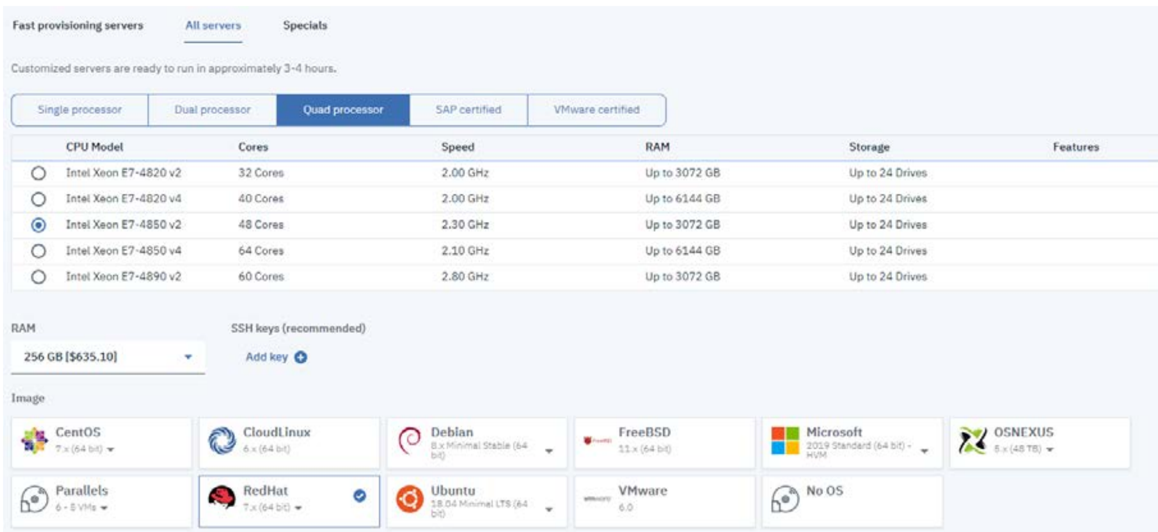
3. From the Bare Metal Server offering details page, select the appropriate quantity of servers and customize the **Hostname** and **Domain** fields. Select the desired billing model (hourly, monthly, or by contract).

4. Select the desired IBM Cloud location. Furthermore, if necessary, select a particular data center for that location for the bare metal server to be deployed. Ideally, an IBM Spectrum Protect server should be deployed close to client resources (data) being protected. When you order IBM Cloud Object Storage, if you select Regional object storage, the storage should be within the same IBM Cloud location as the instance for

optimal throughput (any data center within that same location should suffice).

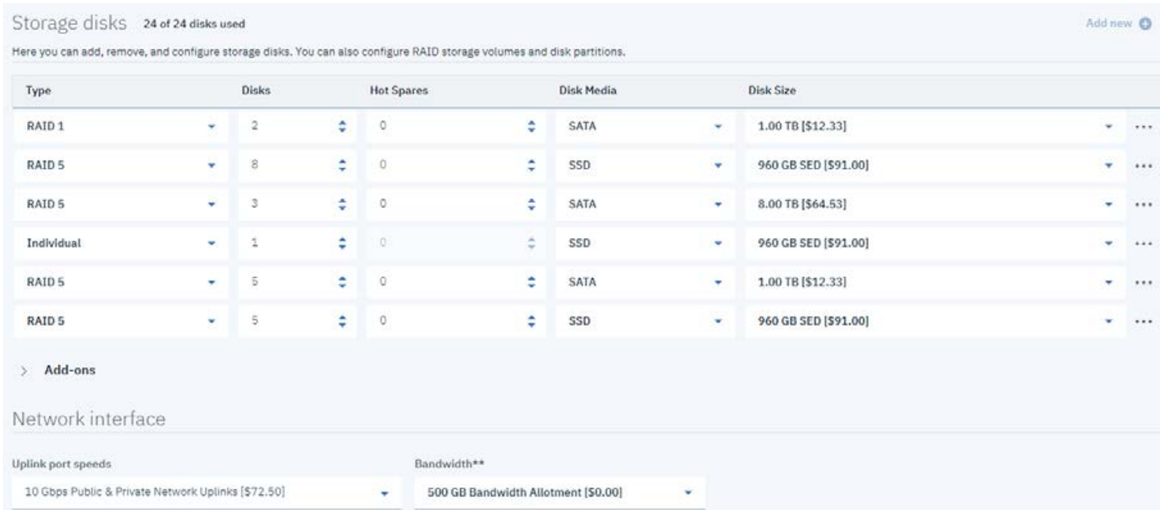


5. Customize the bare metal server instance type. You might have to click the **All Servers** tab to find the preferred servers that are specified in this paper. Adjust the RAM value for the server as necessary because the default memory allotment might not be sufficient. Select the appropriate operating system. A supported version of Red Hat Enterprise Linux or Ubuntu Linux LTS is preferred for IBM Spectrum Protect instances running in IBM Cloud.



6. Configure block storage to Blueprint specifications. For each storage disk line item that is added, the RAID type, number of disks, hot spare coverage, disk media type, and disk size can be selected. For bare metal servers, the IBM Cloud team will ensure that disks are properly installed within the server chassis and RAID configurations are initialized. Ensure that 10 Gbps private network uplinks are selected for the uplink port speeds for large, medium, or small Blueprint systems to ensure adequate throughput

to IBM Cloud Object Storage.

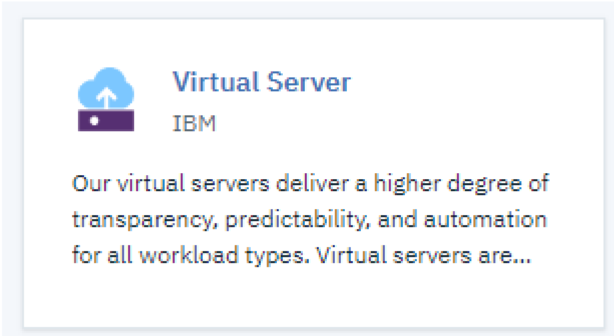


7. Add any desired add-ons and complete the server configuration.
8. Accept the third-party service agreement terms and create the resource or save a quote for later.

IBM Cloud Virtual Servers

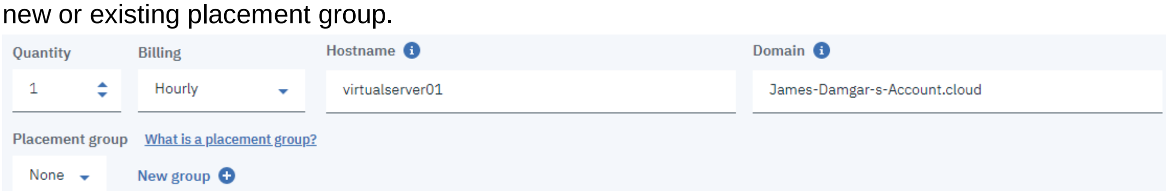
1. At the top-right corner of the window, click **Create resource**.

2. Under the **Compute** section and **Infrastructure** subsection, click **Virtual Server**.



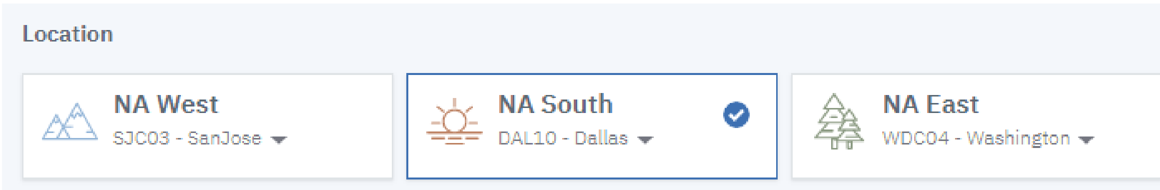
3. Select the appropriate style of virtual server. Avoid the **Transient Virtual Server** option for IBM Spectrum Protect purposes. The **Public Virtual Server** option is much less expensive than the **Dedicated Virtual Server** option because virtual machines are maintained on multitenant hypervisor hosts where resources are shared. For the greatest cost savings for extra-small deployments that will have longevity, choose the **Reserved Virtual Server** option.

4. From the virtual server instance offering details page, select the appropriate quantity of servers and customize the **Hostname** and **Domain** fields. Select the desired billing model (hourly, monthly, or by contract). Virtual machines may be collocated within a new or existing placement group.

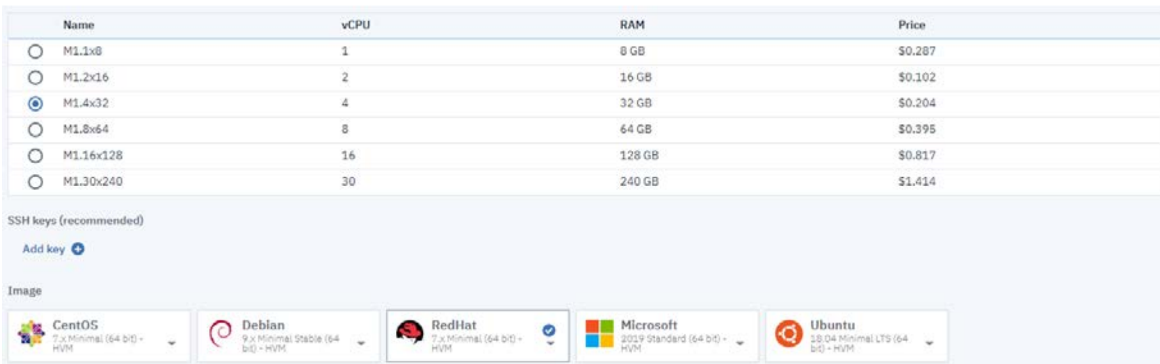


5. Select the desired IBM Cloud location. Furthermore, if necessary, select a particular datacenter for that location for the virtual server to be deployed. Ideally, an IBM Spectrum Protect server should be deployed close to the client resources (data) that

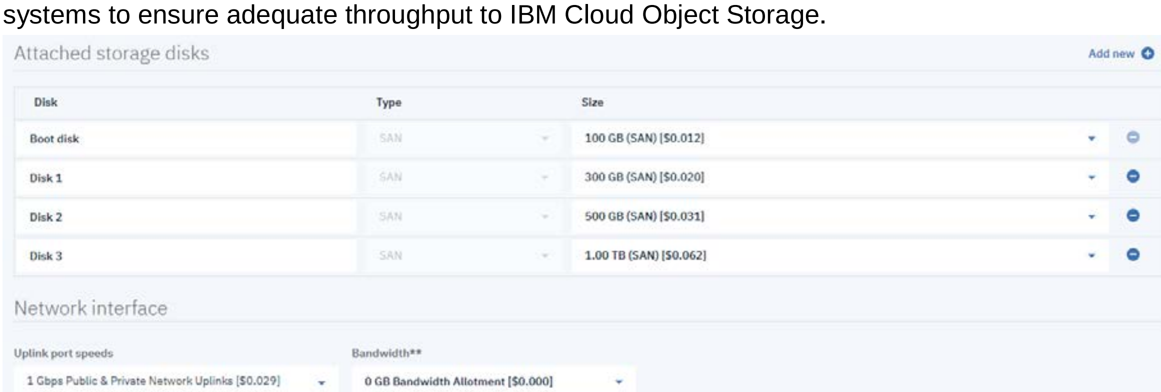
are being protected. If you order IBM Cloud Object Storage with Regional object storage, the Regional storage should be within the same IBM Cloud location as the instance for optimal throughput (any datacenter within that same location should suffice).



6. Customize the virtual server instance type. To find the preferred servers that are specified in this paper, you might have to click the **All Profiles** tab. A supported version of Red Hat Enterprise Linux or Ubuntu Linux LTS is preferred for IBM Spectrum Protect instances running in IBM Cloud.



7. Configure SAN-attached block storage in accordance with Blueprint specifications. For each storage disk line item that is added, you can select a size. Ensure that 1 Gbps private network uplinks are selected for Uplink port speeds for extra-small Blueprint systems to ensure adequate throughput to IBM Cloud Object Storage.



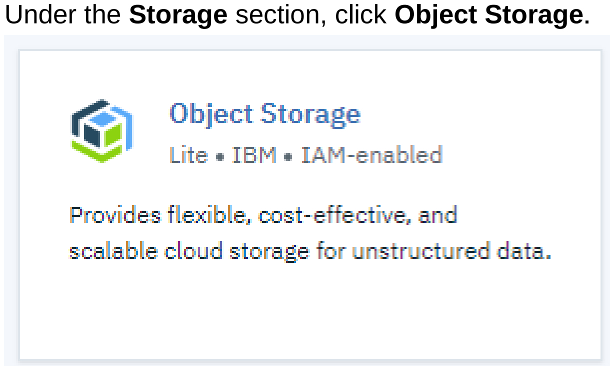
8. Add any desired add-ons and complete the server configuration.

9. Accept the third-party service agreement terms and create the resource or save a quote for later.

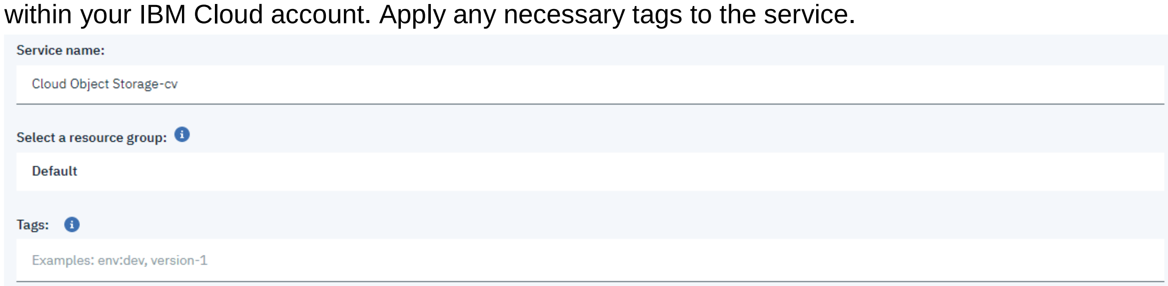
IBM Cloud Object Storage

1. At the top-right corner of the window, click **Create resource.**

2. Under the **Storage** section, click **Object Storage**.

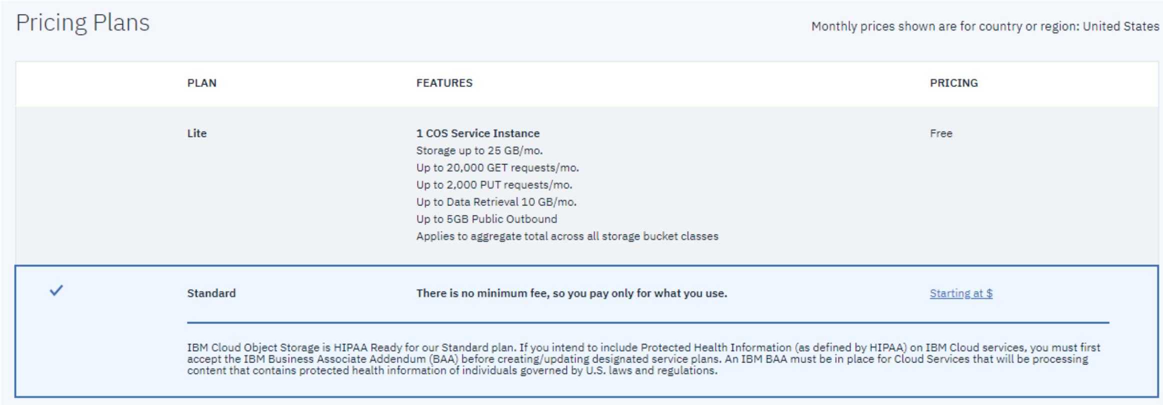


3. Customize the service name for the object storage and an optional resource group within your IBM Cloud account. Apply any necessary tags to the service.



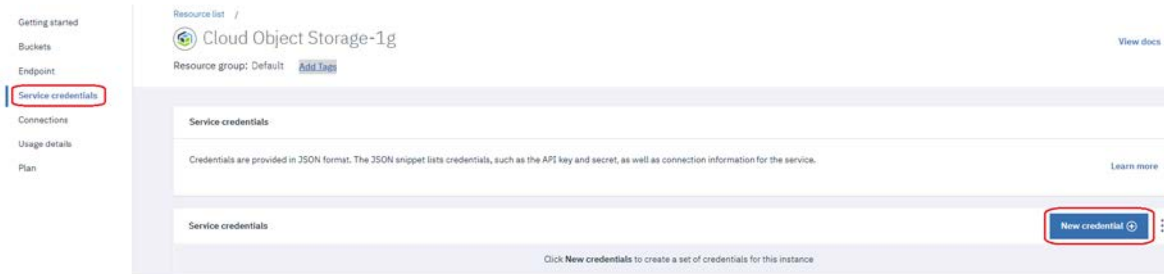
4. For all but the smallest deployments, select a standard pricing plan to ensure necessary capacity and IOPs for IBM Spectrum Protect. To create the object storage

resource, click **Create**.

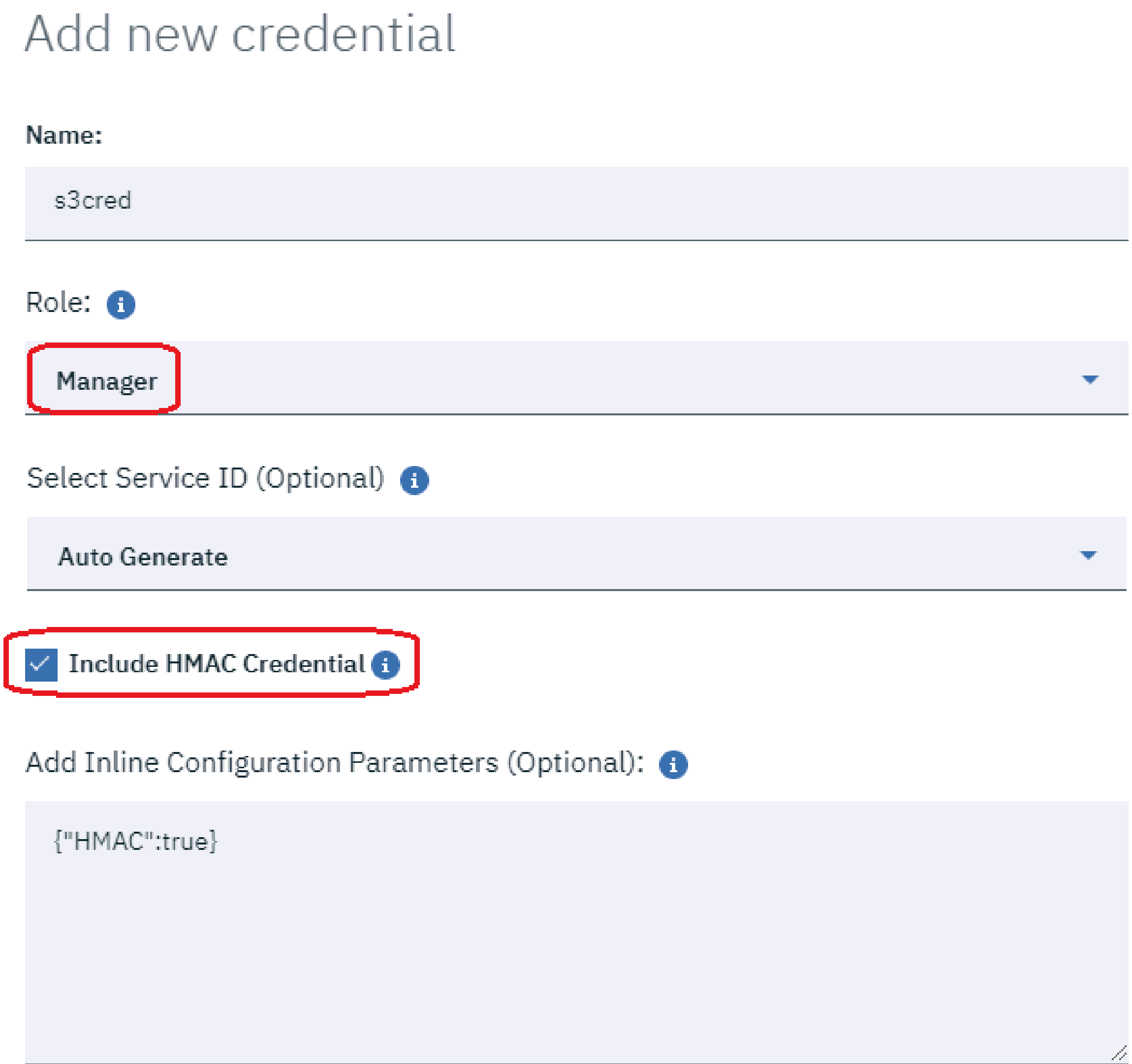


After you create the object storage resource, you must also specify service credentials for the IBM Spectrum Protect server to use for any cloud-container storage pools.

5. On the Cloud Object Storage resource page, navigate to the **Service credentials** tab and click **New credential**.

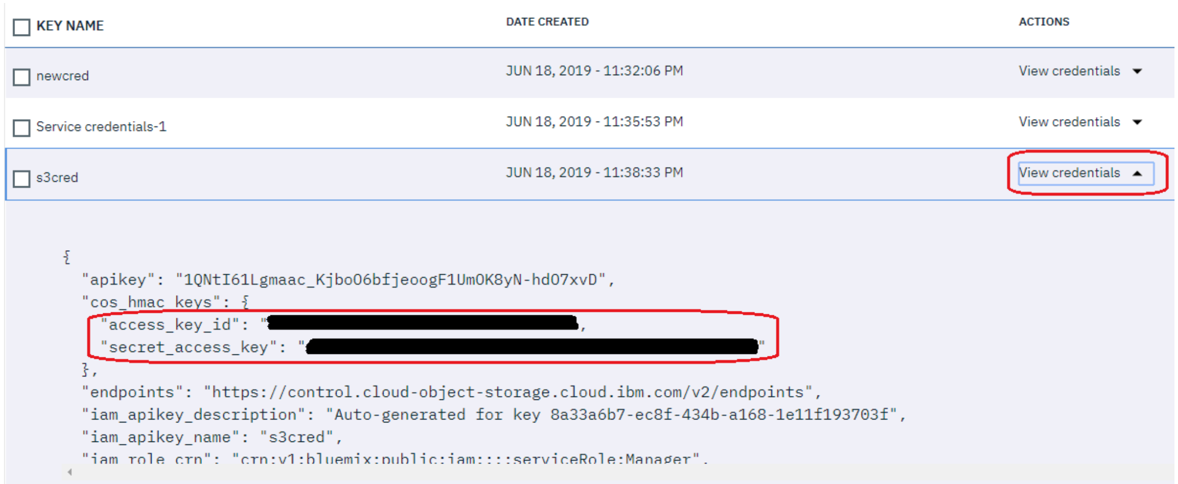


When you add a credential, ensure that the manager role is specified and that the **Include HMAC Credential** check box is selected.



6. In the **ACTIONS** column, click **View credentials** to select a credential name that has HMAC keys. The JSON window that appears will display the public key ("access_key_id") and the private key ("secret_access_key") for S3 protocol object

storage, which is used by IBM Spectrum Protect cloud-container storage pools.



When you access IBM Cloud Object Storage from an IBM Cloud instance, use the optimal S3 protocol endpoint. For a listing of available endpoints, see References [5]. Different endpoints are available, depending on whether the IBM Cloud Object Storage bucket or vault that was created was Regional or Cross-Regional. If possible, use the private endpoint that is geographically closest to the IBM Cloud compute instance to ensure optimal throughput.

References

[1] IBM Spectrum Protect Blueprints:

https://www.ibm.com/developerworks/community/wikis/home?lang=en#!/wiki/Tivoli%20Storage%20Manager/page/IBM%20Spectrum%20Protect%20Blueprints

[2] IBM Cloud, bare metal servers:

https://www.ibm.com/cloud/bare-metal-servers

[3] Overview - IBM Spectrum Protect Supported Operating Systems:

http://www.ibm.com/support/docview.wss?uid=swg21243309

[4] IBM Cloud Object Storage pricing:

https://www.ibm.com/cloud-computing/bluemix/pricing-object-storage

[5] IBM Cloud Object Storage endpoints and storage locations:

https://cloud.ibm.com/docs/services/cloud-object-storage/basics?topic=cloud-object-storage-endpoints

Notices

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

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

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

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

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

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

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

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

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

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

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

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Trademarks